

Trasmissione via PEC

AM/mz

Al Direttore
Dott. Enrico Zola
ARPEA – Agenzia Regionale Per le Erogazioni
in Agricoltura

e, p.c. . Al Responsabile SIRe
Dott.ssa Nicoletta Motta
ARPEA – Agenzia Regionale Per le Erogazioni
in Agricoltura

protocollo@cert.arpea.piemonte.it

Oggetto: Configurazione Tecnico Economica anno 2020 - Trasmissione

Egregio Direttore,

con riferimento all'art. 5 della vigente *“Convenzione quadro per gli affidamenti diretti al CSI-Piemonte per la prestazione di servizi in regime di esenzione IVA”*, Le inviamo in allegato la Configurazione Tecnico Economica contenente la descrizione dei **servizi in continuità** relativi alla sua Agenzia da affidarsi al CSI per l'anno 2020, con i relativi preventivi di costo stimati per ciascuna tipologia di servizio.

Si evidenzia che tali preventivi sono stati valutati sulla base delle indicazioni contenute negli Allegati Tecnici della Convenzione, approvati dal Tavolo di Gestione della Convenzione nella seduta del 18 novembre 2019. I suddetti preventivi tengono conto dei volumi di attività ipotizzati in termini di *effort* annuale previsto per ciascuna figura professionale, oltre che dell'importo e dei volumi per ciascun Servizio IT a misura, dando evidenza della relativa scomposizione in categorie di costo in regime di esenzione IVA.

Si sottolinea, peraltro, che nel contesto della sopra menzionata CTE risultano esplicitate puntualmente, ai sensi dell'art. 20 comma 2 della Convenzione, le misure organizzative, tecniche, procedurali e logistiche relative alla sicurezza nella gestione dei dati personali trattati nell'ambito dei servizi in continuità prestati.



I servizi in questione sono operativi dal 01/01/2020 per cui si auspica che il documento di CTE e il relativo preventivo economico siano approvati in tempi brevi al fine di consentire ad entrambe le Parti di operare nel pieno rispetto delle prescrizioni previste nella Convenzione sottoscritta.

Con l'occasione ci rendiamo disponibili agli approfondimenti siano ritenuti utili e porgiamo cordiali saluti.

Firmato digitalmente
dal Dott. Alessio Mascarello
Funzione organizzativa Attività Produttive,
Ambiente, FPL

108.9,46/2020A

Allegati:

- CTE ARPEA 2020
- CTE ARPEA 2020_figure professionali
- CTE ARPEA 2020_servizi a misura

Rif CSI1010618/00

ARPEA

AGENZIA REGIONALE PIEMONTESE PER LE EROGAZIONI IN AGRICOLTURA

CONFIGURAZIONE TECNICO ECONOMICA

2020

(CTE)

SOMMARIO

| | | |
|----------|---|-----------|
| 1 | GENERALITÀ | 4 |
| 2 | PREMESSA | 6 |
| 3 | VALORIZZAZIONE DEI SERVIZI | 6 |
| 4 | CONDIZIONI DI FORNITURA | 6 |
| 5 | SICUREZZA E PROTEZIONE DEI DATI PERSONALI | 7 |
| 6 | SEGNALAZIONI RECLAMI | 9 |
| 7 | MODALITÀ DI EROGAZIONE DEI SERVIZI | 10 |
| 8 | QUADRO ECONOMICO RIASSUNTIVO DEI SERVIZI | 10 |
| 9 | DETTAGLIO SERVIZI | 10 |
| 9.1 | Servizi IT Trasversali | 12 |
| 9.1.1 | Altri servizi ad hoc..... | 12 |
| 9.1.2 | Asset, Compliance e Security Management..... | 16 |
| 9.1.3 | Governo | 16 |
| 9.1.4 | Supporto specialistico operativo..... | 17 |
| 9.2 | Servizi IT per Aree Logiche Omogenee (ALO) | 17 |
| 9.2.1 | ALO – Comunicazione e accesso | 17 |
| 9.2.2 | ALO – Flussi documentali e dematerializzazione..... | 19 |
| 9.2.3 | ALO – Servizi Contabili | 21 |
| 9.2.4 | ALO – Territorio | 22 |
| 9.2.5 | ALO – Web | 23 |
| 9.3 | Servizi di piattaforma applicativi | 25 |
| 9.3.1 | Contabilità..... | 25 |
| 9.3.2 | Dematerializzazione..... | 27 |
| 9.3.3 | Fatturazione elettronica | 29 |
| 9.3.4 | PEC - Posta Elettronica Certificata | 30 |
| 9.3.5 | Posta Elettronica e servizi di Comunicazione Unificata..... | 33 |
| 9.3.6 | Servizi al Personale | 38 |
| 9.3.7 | Sito Web | 40 |
| 9.3.8 | Telemaco | 42 |
| 9.4 | Servizi di piattaforma infrastrutturali..... | 45 |
| 9.4.1 | Servizi Virtual Data Center | 45 |

| | | |
|-------|--|----|
| 9.4.2 | Servizi di End-Point Management | 56 |
| 9.4.3 | Servizi di Rete e di sicurezza ICT..... | 59 |
| 9.5 | Servizi di piattaforma supporto e cooperazione | 71 |
| 9.5.1 | Automazione processi di input/output | 71 |
| 9.5.2 | Identity & Access | 73 |

1 GENERALITÀ

Denominazione CTE

Configurazione Tecnico Economica – Anno 2020

Ente Committente

Agenzia Regionale Piemontese per le Erogazioni in Agricoltura (ARPEA)

RIFERIMENTI DELL'ENTE

Responsabile della CTE: Nicoletta Motta

Referente Sistema Informativo: Nicoletta Motta

RIFERIMENTI CSI-PIEMONTE

| Servizio IT/Servizio Piattaforma/Aree Logiche Omogenee (ALO) | Nome Cognome |
|--|--------------------|
| ALO – Comunicazione e accesso | Pier Paolo Gruero |
| ALO – Flussi documentali e dematerializzazione | Eugenio Vota |
| ALO – Servizi Contabili | Giuliana Bonello |
| ALO – Territorio | Marco Cavagnoli |
| ALO – Web | Andrea Muraca |
| Asset, Compliance e Security Management | Alessio Mascarello |
| Automazione processi di input/output | Domenico Lucà |
| Contabilia | Giuliana Bonello |
| Dematerializzazione | Eugenio Vota |
| Fatturazione elettronica | Eugenio Vota |
| Governo | Alessio Mascarello |
| Identity & Access | Pier Paolo Gruero |
| PEC - Posta Elettronica Certificata | Pier Paolo Gruero |
| Posta Elettronica e servizi di Comunicazione Unificata | Pier Paolo Gruero |
| Servizi al personale | Cinzia Chiesa |
| Servizi Cloud | Vito Baglio |
| Servizi Contabili | Giuliana Bonello |
| Servizi di Data Center | Vito Baglio |

| Servizio IT/Servizio Piattaforma/Aree Logiche Omogenee (ALO) | Nome Cognome |
|---|---|
| Servizi di End-Point Management | Pier Paolo Gruero |
| Servizi di rete e di sicurezza ICT | Vito Baglio |
| Web | Andrea Muraca |
| Supporto specialistico direzionale | I responsabili delle singole ALO o ambiti |
| Supporto specialistico operativo | I responsabili delle singole ALO |
| Telemaco | Livio Daniele |

Referente cliente

Alessio Mascarello

DOCUMENTI E RIFERIMENTI

- “Convenzione per gli affidamenti diretti al CSI-Piemonte per la prestazione di servizi in regime di esenzione IVA”, approvata con D.G.R. n. 5-8240 del 27/12/2018, valevole dal 01/01/2019 per il triennio 2019-2021
- Catalogo e Listino dei servizi del CSI
- Schede Integrative al Catalogo e Listino dei servizi del CSI
- “Programma pluriennale in ambito ICT” per il triennio 2019-2021, approvato con la Deliberazione della Giunta Regionale del 27 dicembre 2018, n. 4-8239.

2 PREMESSA

La presente proposta di CTE 2020 riguarda i **Servizi in continuità** erogati in regime di esenzione IVA in coerenza con la Convenzione per gli affidamenti diretti al CSI-Piemonte per la prestazione di servizi in regime di esenzione IVA e i relativi Allegati, approvata con D.G.R. n. 5-8240 del 27/12/2018, valevole dal 01/01/2019 per il triennio 2019-2021.

Come di consueto, il Referente cliente (indicato al paragrafo “Riferimenti del CSI-Piemonte”) è a disposizione per integrare o mettere a punto i contenuti della proposta a fronte di necessità non ancora definite.

3 VALORIZZAZIONE DEI SERVIZI

I Servizi valorizzati nel presente documento di CTE sono svolti **in continuità a partire dal 01/01/2020 fino al 31/12/2020**.

Per i servizi oggetto della presente CTE si applica il regime di esenzione IVA, in coerenza con la dichiarazione del possesso dei requisiti previsti per l'applicazione del regime di esenzione IVA di Regione Piemonte prot. N. 00012608/2019 del 07/03/2019. Pertanto, i volumi ivi indicati rappresentano una stima delle attività previste e concordate con la Vostra Direzione di conseguenza la valorizzazione economica è da intendersi come preventivo di costo.

Il dettaglio relativo agli elementi di costo che concorrono alla determinazione del preventivo economico è allegato al presente documento, che costituisce parte integrante e sostanziale della presente proposta.

L'avanzamento delle attività nonché il relativo andamento dei costi saranno monitorati secondo quanto previsto dalla Convenzione citata in premessa.

La rendicontazione finale darà evidenza dei costi sostenuti e quindi determinerà l'eventuale conguaglio.

L'interruzione di uno dei servizi attivati e qui descritti avverrà solo su esplicita comunicazione dell'Ente. In ogni caso, il CSI avrà diritto al pagamento delle spese sostenute per le prestazioni eseguite e/o in corso di esecuzione.

4 CONDIZIONI DI FORNITURA

Per le condizioni di fornitura dei servizi previsti in CTE si fa riferimento a quanto contenuto nella Convenzione citata in Premessa

5 SICUREZZA E PROTEZIONE DEI DATI PERSONALI

I servizi oggetto della presente proposta, comportano un trattamento di dati personali e/o particolari di titolarità del Cliente. In virtù di quanto prevede oggi la normativa in materia di protezione dei dati (Codice Privacy modificato dal d.lgs. 101/2018 e GDPR 2016/679), con l'accettazione della presente proposta il CSI Piemonte assume il ruolo di Responsabile del trattamento. Le modalità di svolgimento delle attività sui trattamenti dati saranno effettuate nel rispetto dei vincoli contenuti nelle prescrizioni dell'art. 28 comma 3 del GDPR.

Di seguito si specifica pertanto quanto segue:

- Contesto generale con indicazione della natura e della finalità del trattamento, del tipo di dati personali e delle categorie di interessati nonché della durata del trattamento (art 28 comma 3): Il trattamento dei dati – personali e sanitari (definiti “particolari” ai sensi dell’art. 9 del GDPR) dettagliato nel presente documento nei singoli servizi - rientra nell’ambito dello svolgimento dei compiti di interesse pubblico o connesso all’esercizio di pubblici poteri tipici della pubblica amministrazione. I riff. puntuali alle normative di riferimento sono nella disponibilità del Cliente e/o Titolare del trattamento nei suoi documenti privacy (es. Registro delle attività di trattamento, informative, ecc). Gli interessati sono le persone fisiche che intendono usufruire di tale servizio. La durata del trattamento è definita con l’accettazione della presente Proposta o nella convenzione generale
- Istruzioni in materia di protezione dei dati (art 28 comma 3 punti a) - h) GDPR): Tutte le specifiche contenute nel presente documento sono concordate e condivise con il Cliente e rappresentano - tutte - anche le “istruzioni” in materia di protezione dei dati personali.
- Misure organizzative, tecniche, procedurali e logistiche sulla sicurezza nei trattamenti: Per garantire la disponibilità, la riservatezza, l’integrità e la tutela dei dati degli interessati che utilizzeranno tali servizi, ai fini di mitigare i seguenti rischi:
 - distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati;
 - trattamento dei dati non consentito o non conforme alle finalità delle operazioni di trattamento;
 - interruzione della disponibilità dei dati involontaria o volontaria (dolosa);
 - sono implementate le misure di seguito elencate, scelte tenendo conto dello stato dell’arte e dei costi di attuazione, nonché della natura, dell’oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche:

Misura di sicurezza organizzative

| | |
|-------------------|--|
| Formazione | Esistenza di un piano di formazione in materia di protezione dei dati per il trattamento. Esecuzione degli interventi formativi previsti |
|-------------------|--|

| | |
|--|---|
| Istruzioni per il trattamento (ex Disciplinare) | Esistenza di un documento che contenga regole da applicare per il trattamento (principi, regole da applicare nel trattamento, procedure, linee guida, manuali di organizzazione del servizio ecc. ...) Esistenza di procedure/istruzioni che descrivono la gestione degli incidenti che possano comportare violazione di dati personali (data breach) |
| Regole di archiviazione | Sono definiti la politica e i processi di gestione dell'archivio cartaceo consegna, archiviazione, consultazione etc.) |
| Modello organizzativo | Regole e responsabilità a livello aziendale (es codice etico) e a livello di ruoli e responsabilità del progetto o servizio |
| Audit interni | Effettuazione di un audit interno sul trattamento entro 1 anno solare dalla ultima valutazione (o dalla messa in esercizio del software/attivazione del servizio) |
| Audit esterni | Effettuazione di un audit esterno sul trattamento entro 1 anno solare dalla ultima valutazione (o dalla messa in esercizio del software/attivazione del servizio) |
| Misure contratti | Predisposizione di contratti passivi che includano le clausole privacy definite a livello aziendale per il rispetto del GDPR. Clausole e condizioni di dettaglio specifiche per il trattamento |
| presidio del ciclo di vita del sw | Sono predisposti e aggiornati i documenti di progettazione, architettura, installazione del software utilizzato (es vista d'insieme, documento di architettura, deploy, ...) |

Misure di sicurezza tecniche trasversali:

| | |
|---|--|
| Armadi e contenitori dotati di serrature | Conservazione sicura dei documenti cartacei e backup |
| Armadi e contenitori ignifughi | Conservazione sicura dei documenti cartacei e backup |
| Cassaforte ignifuga | Conservazione sicura dei documenti cartacei e backup |
| Misure antincendio | Misure di protezione dei beni e dei documenti |
| Sistemi di sorveglianza | Misure di controllo accessi ai locali |
| Gestione delle postazioni di lavoro | Misure adottate per ridurre la possibilità che le postazioni di lavoro (sistemi operativi, applicazioni aziendali, software per ufficio, impostazioni etc.) vengano sfruttate per violare la sicurezza dei dati personali (es., ...) |

| | |
|---|--|
| Utilizzo di infrastrutture sicure (hw e complementari) | manutenzione fisica degli apparati IT e dei sistemi complementari (es. utilizzo infrastrutture in sala CED per ospitare i servizi applicativi erogati e i dati, utilizzo di protocolli di accesso sicuri) |
| Infrastrutture logiche (ex patch di sistema) | utilizzo di sistemi aggiornati (es middleware, software dei sistemi, ...) |
| Antivirus | installazione di antivirus aggiornato sulle postazioni di lavoro |
| DLP (Data Loss Prevention) | utilizzo di sistemi di DLP per evitare la trasmissione di dati personali o riservati dalle postazioni |
| Network monitoring | strumenti di packet filtering |
| Business continuity/disaster recovery | esistenza di procedure per garantire la BC e/o il DR |
| Separazione LAN | separazione LAN ambienti sviluppo, test, collaudo e produzione |
| Protezione della navigazione web | utilizzo sistemi di web filtering |
| VPN | utilizzo di VPN per l'accesso alle risorse da remoto |
| Protezione perimetrale (firewall) | strumenti di protezione della rete |
| Protezione applicativa (WAF WEB Application Firewall) | strumenti di protezione degli applicativi WEB |
| Gestione Log accessi privilegiati (SIEM) | strumenti per la gestione dei log dei sistemi. (es log dei server dei database, dei firewall, etc). Tali strumenti permettono di correlare su più fonti un accadimento, es un accesso illecito da un ip , posso andare a vedere su tutti i log di tutti gli apparati tracciati cosa e avvenuto, etc) |
| Backup e restore | Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup |

Tali misure organizzative, dovranno essere verificate e valutate periodicamente qualora si ravveda una variazione dell'efficacia delle stesse o del livello di rischio iniziale. Le eventuali misure tecniche sono esplicitate nei capitoli relativi ai servizi erogati.

6 SEGNALAZIONI RECLAMI

Nel caso in cui il responsabile della CTE volesse inoltrare una segnalazione o un reclamo, previa verifica con i referenti clienti di cui al precedente capitolo 1, occorrerà inviare una comunicazione

riportante in oggetto la dicitura “Segnalazione” o "Reclamo", seguita da una breve descrizione, alla casella PEC: protocollo@cert.csi.it e agli stessi referenti.

7 MODALITÀ DI EROGAZIONE DEI SERVIZI

Per quanto attiene le modalità di erogazione dei servizi previsti in CTE (orari, modalità di accesso, utenti abilitati) si fa riferimento a quanto espresso nei paragrafi seguenti riferiti ai singoli servizi applicativi e servizi di piattaforma.

Pur essendo i servizi informatici disponibili h24 7x7 (ovvero l’accesso alle applicazioni software), al di fuori degli orari di erogazione dei servizi eventuali disservizi o interruzioni che potranno verificarsi saranno presi in carico a partire dal successivo orario di erogazione dei servizi.

8 QUADRO ECONOMICO RIASSUNTIVO DEI SERVIZI

| ARPEA | Importo |
|----------|--------------|
| CTE 2020 | € 347.954,67 |

*Il totale è comprensivo degli eventuali oneri per la sicurezza.
Salvo conguaglio a fine esercizio.*

9 DETTAGLIO SERVIZI

| Servizio a Catalogo | Importo Totale |
|---|----------------|
| Servizi IT | |
| Altri servizi ad hoc | € 85.101,49 |
| Asset, Compliance e Security Management | € 971,00 |
| Governare | € 55.472,00 |
| Supporto specialistico operativo (Attività di presidio) | € 17.462,40 |
| Supporto specialistico operativo (Servizio di Disaster Recovery e test) | € 12.378,00 |
| Servizi IT per ALO – Comunicazione e accesso | |
| Gestione operativa applicazioni - Assistenza funzionale | € 728,50 |
| Servizi IT per ALO – Flussi documentali e dematerializzazione | |
| Supporto specialistico direzionale | € 2.020,00 |
| Servizi IT per ALO – Servizi Contabili | |
| Supporto specialistico direzionale | € 2.020,00 |

| | |
|--|---------------------|
| Servizi IT per ALO – Territorio | |
| Elaborazione, integrazione e gestione dati e contenuti | € 1.297,50 |
| Servizi IT per ALO – Web | |
| Elaborazione, integrazione e gestione dati e contenuti | € 1.794,00 |
| Servizi di Piattaforma Applicativi | |
| Contabilità | € 5.500,00 |
| Dematerializzazione | € 46.535,62 |
| Fatturazione elettronica | € 669,60 |
| PEC - Posta Elettronica Certificata | € 504,43 |
| Posta Elettronica e servizi di Comunicazione Unificata | € 4.634,40 |
| Servizi al Personale | € 3.792,12 |
| Sito Web | € 2.940,00 |
| Telemaco | € 1.403,50 |
| Servizi di Piattaforma Infrastrutturali | |
| Virtual Data Center | € 37.337,77 |
| Servizi di End-Point Management | € 51.438,43 |
| Servizi di Rete e di Sicurezza ICT | € 11.938,39 |
| Servizi di Piattaforma Supporto e Cooperazione | |
| Automazione processi di input/output | € 120,00 |
| Identity & Access | € 1.895,52 |
| TOTALE SERVIZI | € 347.954,67 |

*Il totale è comprensivo degli eventuali oneri per la sicurezza.
 Salvo conguaglio a fine esercizio.*

9.1 SERVIZI IT TRASVERSALI

9.1.1 ALTRI SERVIZI AD HOC

Nel presente paragrafo sono descritti e preventivati servizi che presentano una specifica composizione dei costi e delle attività non desumibile dal documento “Catalogo e listino dei servizi del CSI”, allegato alla Convenzione citata in premessa.

Preventivo economico:

| Servizio IT | Importo Totale | Servizi professionali | Servizi a metrica | Acquisti dedicati | Quote d'uso sw/hw |
|--|--------------------|-----------------------|-------------------|-------------------|-------------------|
| Acquisto linee dati SCR | € 9.726,49 | | | € 9.726,49 | |
| Flussi stampe massive | € 12.264,00 | € 12.264,00 | | | |
| Gestione rete fonia dati | € 14.959,72 | € 11.005,00 | | € 3.954,72 | |
| Manutenzione HW | € 3.501,28 | | | € 3.501,28 | |
| DPS, Vulnerability Assessment, Supporto a ISO27000 | € 42.960,00 | € 17.280,00 | | € 25.680,00 | |
| Manutenzione e gestione sala di contingency | 1.690,00 | 0 | | 1.690,00 | |
| TOTALE | € 85.101,49 | € 40.549,00 | - | 44.552,49 | - |

Descrizione dei servizi IT erogati

ACQUISTO LINEE DATI SCR

Il servizio di connettività offerto garantisce:

- Collegamenti da e verso Internet, attraverso gli accessi/link multicarrier del CSI;
- Collegamenti verso i servizi della PA centrale e le altre Regioni attraverso la rete SPC;
- Prevede la fornitura e il monitoraggio di un collegamento in fibra ottica di tipo C3 per la sede di via Bogino 23 e dei collegamenti per il telelavoro dei seguenti dipendenti:

| Dipendente | Tipologia | Indirizzo | Città |
|-------------------------------|-----------|---------------------|-------------------|
| Ivan Alessio | B1 | Via Marconi, 25/2 | Rivalta di Torino |
| Marta Marchese | B1 | Via I maggio, 70 | Canelli |
| Federica Rea | B1 | Via Montegrappa, 38 | Chivasso |
| Luigi Varvelli | B1 | Corso Cavour, 70 | Trino |
| Giulia Manissero | B1 | Via Don Milani 6 | Carmagnola |
| Maria Veronica Basualdo | B1 | Via Vittoria 14 | Torino |
| Collegamento principale | C4 | Via Bogino | Torino |
| Trasloco Gassino - Carmagnola | B1 | | |

TRATTAMENTO DEI DATI PERSONALI:

Non applicabile.

MODALITÀ DI EROGAZIONE DEL SERVIZIO

I servizi di rete sono disponibili H24 7 giorni su 7. L'orario di erogazione dei Servizi di assistenza è il seguente:

| Servizio | Lunedì - Giovedì | Venerdì |
|-------------------|--------------------------------|--------------------------------|
| hd_agenzie@csi.it | 09.00 - 12.30 13.30 - 17.00 | 09.00 - 12.30 13.30 - 16.00 |

FLUSSI STAMPE MASSIVE

Il servizio tratta la gestione dei flussi informativi per la produzione delle stampe massive necessarie all'attività svolta dall'Ente. Per l'anno 2020 sono stati previsti 7 flussi massivi da gestire.

TRATTAMENTO DEI DATI PERSONALI:

Le informazioni non sono ancora disponibili al momento della stesura del documento. Saranno prodotte all'occorrenza.

GESTIONE RETE FONIA DATI

Il Servizio offerto da CSI nell'ambito della Convenzione garantisce:

- la connettività da e verso Internet alla rete aziendale e la connettività interna;
- la raggiungibilità di servizi di server-farm;
- la gestione e manutenzione della rete LAN dedicata e degli apparati attivi, comprensivo del rateo di ammortamento;
- il servizio di accesso ad Internet in modalità Wi-Fi per i dipendenti dell'Ente. Nel corso dell'anno è prevista la messa a disposizione del servizio di accesso Wi-Fi dedicato agli ospiti di ARPEA di cui nel seguito si riepilogano le caratteristiche principali:

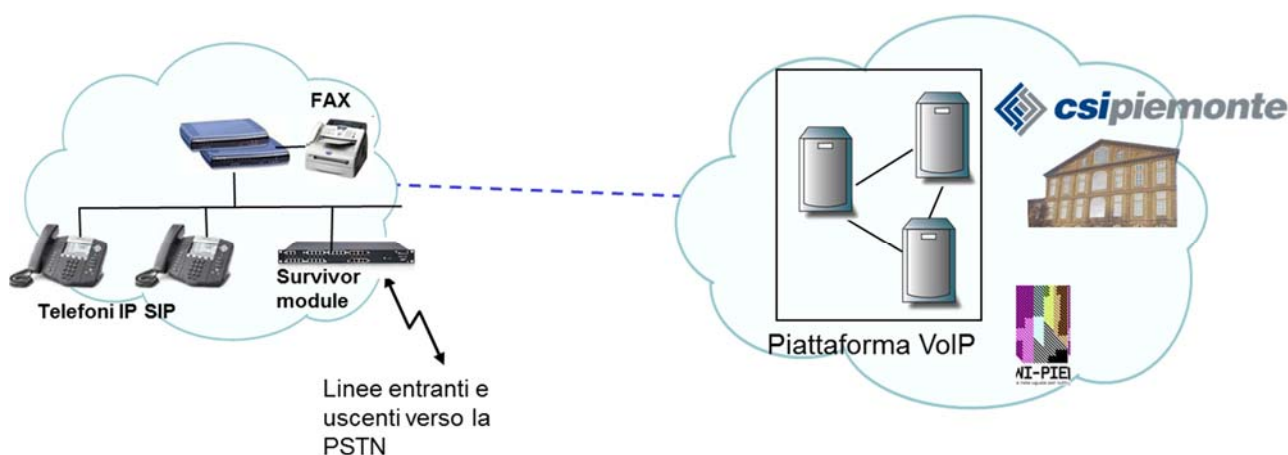
- Self Provisioning delle credenziali, a mezzo del quale un utente in possesso di una SIM rilasciata da operatori italiani può registrarsi (Una Tantum) e ottenere la coppia user/password per l'accesso al servizio. Durante la fase di registrazione, oltre a fornire nome, cognome e e-mail, l'utente dovrà effettuare una chiamata dal proprio cellulare ad un numero verde per la conferma del numero di telefono e la sua acquisizione nel sistema;
- Le credenziali non hanno scadenza (salvo il mancato utilizzo per un certo numero di mesi) e la navigazione, senza limiti di durata, è sottoposta a URL Filtering. Fornitore del servizio e Titolare del trattamento dei dati è il CSI Piemonte;
- Il servizio è erogabile utilizzando l'infrastruttura wireless già nella disponibilità di ARPEA in quanto gli Access Point possono annunciare due SSID differenti. Naturalmente, gli utenti del servizio Ospiti non avranno la possibilità di accedere alla LAN di ARPEA.

L'infrastruttura server del servizio di comunicazione VoIP erogato è costituita da **due server virtuali** ospitati sulla Virtual Farm del CSI-Piemonte e da un apparato gateway Audiocodes Median1000 installato presso la sede di ARPEA. Quest'ultimo apparato permette l'interconnessione VoIP con le linee PSTN PRI dell'ente e per il collegamento dei terminali FAX.

Sui server centrali è presente, in logica cluster, la **piattaforma VoIP Open Source SipXecs** sviluppata e supportata dalla *Community SipFoundry*.

SipXecs è una soluzione Enterprise PBX VoIP fondata nativamente sul protocollo SIP (SSOA: SIP Service Oriented Architecture), completa di tutte le più comuni funzionalità dei tradizionali centralini telefonici. SipXecs è un software sviluppato su sistema operativo Linux (CentOS e altri) e non richiede particolare hardware per l'installazione.

Completamente basato su standard SIP è stato sviluppato nell'ottica di essere interoperabile con tutti i device o le applicazioni di terze parti che implementino tale standard.



I servizi di gestione sistemistica prevedono le seguenti attività:

- gestione da remoto dei profili utente;
- assistenza specialistica di secondo livello;

- gestione sistemistica dell'infrastruttura server e della piattaforma SipXecs;
- gestione sistemistica e manutenzione degli apparati gateway;
- gestione e manutenzione dei due posti operatore.

MANUTENZIONE HW

Il servizio si applica alle postazioni di lavoro, stampanti ed apparecchiature, identificate da un numero di censimento e che sono presenti all'interno del database dell'asset management.

Il servizio comprende la sostituzione delle parti hardware guaste ed in caso di materiali di consumo (come per es. fusori, toner, ecc) viene emesso un preventivo che dovrà essere autorizzato dall'ente prima della sostituzione del pezzo.

Per la corretta erogazione del servizio è necessario che il CSI-Piemonte abbia a disposizione l'asset dell'ente e che gli vengano comunicati eventuali aggiornamenti o spostamenti di tale postazioni in sedi differenti.

È possibile accedere al servizio di assistenza hardware utilizzando i canali utilizzati per richiedere l'assistenza software alle postazioni di lavoro.

TRATTAMENTO DEI DATI PERSONALI:

Non applicabile.

MODALITÀ DI EROGAZIONE DEL SERVIZIO

I servizi di rete sono disponibili H24 7 giorni su 7. L'orario di erogazione dei Servizi di assistenza è il seguente:

| Servizio | Lunedì - Giovedì | Venerdì |
|-------------------|--------------------------------|--------------------------------|
| hd_agenzie@csi.it | 09.00 - 12.30 13.30 - 17.00 | 09.00 - 12.30 13.30 - 16.00 |

DPS, VULNERABILITY ASSESSMENT, SUPPORTO A ISO27000

In considerazione degli obblighi di controllo cui ARPEA è soggetto nel tempo da parte di Commissioni Europee o Ministeriali Italiane, CSI Piemonte è interessato in conseguenza delle forniture prestate e dei servizi gestiti per conto di ARPEA. Ne consegue quindi per parte CSI Piemonte l'impegno di risorse necessarie per corrispondere alle richieste dei certificatori.

Per la realizzazione dell'analisi dello stato della sicurezza e la definizione di un piano di interventi operativi sono previste le seguenti attività:

- Attività di supporto per la conferma della certificazione ISO 27001:2013 : in previsione degli audit che verranno effettuati a norma dell'art. 47, paragrafo 1, del regolamento (UE) n.1306/2013 con lo scopo di esaminare se l'Organismo pagatore soddisfa i criteri di riconoscimento in materia di sicurezza dei sistemi d'informazione definiti dal Regolamento UE 907/2014, e in previsione della verifica annuale per la conferma della certificazione, prevista dall'ente certificatore, occorre svolgere le seguenti attività basate sull'applicazione della norma ISO 27001:2013

- Definizione di un piano di interventi finalizzati alla risoluzione di eventuali non conformità evidenziate dall'attività di assessment svolte dall'ente certificatore e dagli enti di controllo delle attività di ARPEA;
- Individuazione di eventuali punti di debolezza nella gestione e nell'organizzazione della Sicurezza delle componenti di servizio predisposte e gestite da parte di CSI Piemonte;
- Formazione nuovi utenti ARPEA su ISO 27001:2013;
- Effettuare visite ispettive di controllo presso alcuni CAA;
- Supporto ad ARPEA per confermare la certificazione ISO 27001:2013;

A tal fine sarà necessaria la revisione di tutti i processi che compongono il Sistema di Gestione della Sicurezza delle Informazioni, con particolare attenzione alla redazione dei seguenti documenti:

- analisi dei rischi;
- piano di trattamento dei rischi;
- manuale SGSI;
- politica di sicurezza;
- riesame della direzione;
- statement of applicability;
- documenti che descrivono i processi di ARPEA;

Gli obiettivi principali del Vulnerability Assessment sono:

- assicurare che la rete e i sistemi non siano vulnerabili;
- garantire che i dati in rete non siano compromissibili;
- provvedere affinché la sicurezza perimetrale sia correttamente configurata;
- aggiornare opportunamente i sistemi;
- gestire correttamente l'infrastruttura ed evitare anomalie.

TRATTAMENTO DEI DATI PERSONALI

Le informazioni non sono ancora disponibili al momento della stesura del documento. Saranno prodotte all'occorrenza.

9.1.2 ASSET, COMPLIANCE E SECURITY MANAGEMENT

Per la descrizione del servizio fare riferimento al documento "Catalogo e listino dei servizi del CSI"

Preventivo economico:

| Servizio IT | Importo Totale | Servizi professionali | Acquisti dedicati |
|---|-----------------------|------------------------------|--------------------------|
| Asset, Compliance e Security Management | € 971,00 | €971,00 | - |

9.1.3 GOVERNO

Per la descrizione del servizio fare riferimento al documento "Catalogo e listino dei servizi del CSI".

Preventivo economico:

| Servizio IT | Importo Totale | Servizi professionali |
|-------------|----------------|-----------------------|
| Governo | € 55.472,00 | € 55.472,00 |

9.1.4 SUPPORTO SPECIALISTICO OPERATIVO

Sulla base di quanto previsto nel documento “Catalogo e listino dei servizi del CSI”, nel seguito viene fornita la descrizione delle attività previste.

Preventivo economico:

| Servizio IT | Importo Totale | Servizi professionali |
|---|--------------------|-----------------------|
| Supporto specialistico operativo (Presidio) | € 17.462,40 | € 17.462,40 |
| Supporto specialistico operativo (Servizio di Disaster Recovery e test) | € 12.378,00 | € 12.378,00 |
| TOTALE | € 29.840,40 | € 29.840,40 |

Le attività di supporto specialistico operativo riguardano il presidio della logica applicativa, la gestione e analisi dei dati di utilizzo del sistema, il supporto specialistico organizzativo/normativo volto alla definizione dei processi interni all'Ente e alla loro applicazione nel sistema.

In tale servizio rientrano anche il supporto in presidio e le attività di mantenimento e gestione del servizio di Disaster Recovery (ad esclusione dei costi della sala di contingency prevista nei servizi ad hoc).

9.2 SERVIZI IT PER AREE LOGICHE OMOGENEE (ALO)

9.2.1 ALO – COMUNICAZIONE E ACCESSO

Preventivo economico:

| Servizio IT | Importo Totale | Servizi professionali | Servizi a metrica | Acquisti dedicati |
|---|-----------------|-----------------------|-------------------|-------------------|
| Gestione operativa applicazioni – Assistenza funzionale | € 728,50 | € 728,50 | - | - |
| TOTALE | € 728,50 | € 728,50 | - | - |

DESCRIZIONE DEI SERVIZI IT EROGATI

Il servizio comprende tutte le attività di gestione dell'identità digitale di un utente; in particolare rientrano in tale voce: rilascio di utenze; rilascio di certificati digitali; revoca delle credenziali; modifica degli attributi dell'identità (e-mail, CF, Ente di appartenenza); gestione malfunzionamenti delle credenziali.

TRATTAMENTO DEI DATI PERSONALI:

| Misura verticale | Descrizione |
|---|---|
| Minimizzazione della quantità dei dati personali | rientrano misure di filtraggio e rimozione, riduzione della sensibilità attraverso la conversione, ridurre la natura identificativa del dato, ridurre l'accumulazione dei dati, limitare l'accesso ai dati |
| Profilazione | utilizzo di sistemi di profilazione con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di profilazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Autenticazione (ex autenticazione centralizzata) | utilizzo di sistemi di autenticazione (locali o nazionali) con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di autenticazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Utilizzo di sistemi di autenticazione multifattore | E' previsto l'uso di certificati digitali, PIN, o autenticazione per l'autenticazione dell'utente e/o per i servizi di cooperazione applicativa |
| Gestione del ciclo di vita delle credenziali (ex scadenza credenziali) | gestione del ciclo del provisioning delle credenziali di autenticazione e della profilazione, in particolare della scadenza della credenziale (anche in termini di gestione delle segnalazioni da sistemi centralizzati) |
| Tracciabilità accessi risorse (ex tracciabilità accessi DB e audit log applicativi) | possibilità di tracciare accessi alle risorse critiche (es DB, front end e back end del servizio, share di rete critici) |
| Audit log applicativi | nel DB è prevista la tracciatura dell'identificativo utente che ha inserito/modificato i dati delle tabelle e si è in grado di risalire a chi e quando ha inserito/modificato/cancellato il record |
| Abilitazioni puntuali accessi DB (proxy SQL) | utilizzo di proxy SQL |
| Minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento (ex scansione vulnerabilità) | (es politiche di aggiornamento del software, test funzionale e di vulnerabilità del software utilizzato, limitazioni dell'accesso fisico al materiale che contiene dati personali,) |

| | |
|--|--|
| Cifratura del dato | mezzi implementati per assicurare la confidenzialità dei dati archiviati (in database, file, backup etc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di compromissione etc.) |
| Cifratura del canale | Applicazione di canale cifrato per le comunicazioni mediante utilizzo di protocolli HTTPS e SSH |
| Pseudonimizzazione | adozione di tecniche che garantiscono la non attribuzione a una persona identificata o identificabile di un dato ma consentono di identificare in un secondo momento i dati anche in maniera indiretta o da remoto (es conservando separatamente le informazioni che permettono di associare la persona al dato) |
| Backup e restore | Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup |
| Backup cifrati | utilizzo di sistemi per la cifratura dei backup |
| Business continuity/disaster recovery | esistenza di procedure per garantire la BC e/o il DR |

UTENTI ABILITATI AL SERVIZIO

Dipendenti e collaboratori dell'Ente

MODALITÀ DI ACCESSO AL SERVIZIO

n.a.

MODALITÀ DI EROGAZIONE DEL SERVIZIO

Il servizio viene attivato con l'invio della richiesta scritta da parte dell'utente contenente i dati personali alla casella hd_agenzie@csi.it con l'elenco degli applicativi/funzionalità a cui deve essere abilitato.

La richiesta deve essere preventivamente autorizzata da un funzionario responsabile.

Il servizio si conclude con l'invio all'utente delle sue credenziali o con la comunicazione all'utente dell'avvenuta attività.

Le credenziali vengono erogate secondo quanto previsto dal Documento Programmatico sulla Sicurezza del CSI Piemonte, che prevede l'emissione in modalità sicura secondo i seguenti criteri:

- la credenziale viene generata con password di 16 caratteri alfanumerici maiuscoli e generati secondo algoritmo casuale;
- la password viene generata scaduta ed indicato all'utente di cambiarla al primo accesso;
- la password viene distribuita metà in busta chiusa riservata personale e metà via email alla casella istituzionale dell'utente.

9.2.2 ALO – FLUSSI DOCUMENTALI E DEMATERIALIZZAZIONE

Preventivo economico:

| Servizio IT | Importo Totale | Servizi professionali | Servizi a metrica | Acquisti dedicati |
|------------------------------------|-------------------|-----------------------|-------------------|-------------------|
| Supporto specialistico direzionale | € 2.020,00 | € 2.020,00 | - | - |
| TOTALE | € 2.020,00 | € 2.020,00 | - | - |

DESCRIZIONE DEI SERVIZI IT EROGATI

Rientrano nelle attività di supporto specialistico direzionale, le richieste di consulenza ad alto livello sull'uso del sistema e delle sue componenti, il supporto all'interpretazione ed applicazione delle norme specifiche in materia digitale, con particolare riferimento alla coerenza tra digitalizzazione dei processi ed il rispetto delle norme che regolano gli iter amministrativi, il supporto inerente specifiche tematiche riconducibili alla dematerializzazione in relazione ai processi, ai dati, alle attività, ai sistemi ed agli strumenti utilizzati. Nella fattispecie il servizio è indirizzato a supportare l'Ente in materia di gestione dei flussi documentali e della dematerializzazione.

Utenti abilitati al servizio

Dipendenti dell'Ente.

Modalità di accesso

n.a.

Modalità di erogazione

A chiamata.

9.2.3 ALO – SERVIZI CONTABILI

Preventivo economico:

| Servizio IT | Importo Totale | Servizi professionali | Servizi a metrica | Acquisti dedicati |
|------------------------------------|-------------------|-----------------------|-------------------|-------------------|
| Supporto specialistico direzionale | € 2.020,00 | € 2.020,00 | - | - |
| TOTALE | € 2.020,00 | € 2.020,00 | - | - |

Descrizione dei servizi IT erogati

Attività di supporto all'Ente sui temi dello sviluppo ed impiego delle tecnologie digitali nell'ambito dei sistemi contabili, come ad esempio:

- consulenza ad alto livello sull'uso del sistema e delle sue componenti, o in relazione a processi che presuppongono la conoscenza della relativa tematica;
- supporto all'interpretazione ed applicazione delle norme specifiche in materia digitale, con particolare riferimento alla coerenza tra digitalizzazione dei processi e rispetto delle norme che regolano gli iter amministrativi nelle diverse materie di competenza dell'Ente;
- supporto per l'attuazione delle politiche di cooperazione inter-ente al fine di avviare iniziative di riuso di applicazioni specifiche.

Utenti abilitati al servizio

Dipendenti e collaboratori dell'Ente.

Modalità di accesso

n.a.

Modalità di erogazione

A chiamata.

9.2.4 ALO – TERRITORIO

Preventivo economico:

| Servizio IT | Importo Totale | Servizi professionali | Servizi a metrica | Acquisti dedicati |
|--|-------------------|-----------------------|-------------------|-------------------|
| Elaborazione, integrazione e gestione dati e contenuti | € 1.297,50 | € 1.297,50 | - | - |
| TOTALE | € 1.297,50 | € 1.297,50 | - | - |

DESCRIZIONE DEI SERVIZI IT EROGATI

Il servizio *Elaborazione, integrazione e gestione dati e contenuti* in questo contesto tratta le informazioni necessarie per assolvere al debito informativo verso ANAC in ottemperanza della Legge 190/2012.

TRATTAMENTO DEI DATI PERSONALI:

- Tipologia di dati che il servizio tratta: dati personali (dati anagrafici e codice fiscale) di soggetti ai quali sono conferiti incarichi, trattati per adempimenti L.190/212 e normativa sulla trasparenza (che prevede la pubblicazione degli stessi dati sul sito dell'Ente).
- Tempo di conservazione dei dati: tempo richiesto per la elaborazione e produzione dei dati necessari per l'adempimento.
- Tempo di conservazione dei log di accesso o traffico: n.a.
- Ulteriori misure tecniche di sicurezza applicate: n.a.

UTENTI ABILITATI AL SERVIZIO

n.a.

MODALITÀ DI ACCESSO AL SERVIZIO

n.a.

MODALITÀ DI EROGAZIONE DEL SERVIZIO

Attivato all'occorrenza contattando direttamente il referente.

9.2.5 ALO – WEB

Preventivo economico:

| Servizio IT | Importo Totale | Servizi professionali | Servizi a metrica | Acquisti dedicati |
|--|-------------------|-----------------------|-------------------|-------------------|
| Elaborazione, integrazione e gestione dati e contenuti | € 1.794,00 | € 1.794,00 | - | - |
| TOTALE | € 1.794,00 | € 1.794,00 | - | - |

Descrizione dei servizi IT erogati

L'ALO - Web si colloca nello scenario più generale delle attività di comunicazione, sia interna che esterna, degli Enti consorziati. Obiettivo primario del servizio è supportare gli Enti nella comunicazione on line verso la propria utenza di riferimento: cittadini, imprese, professionisti, altri Enti e dipendenti della PA. Il servizio di *Elaborazione, integrazione e gestione dati e contenuti* tratta l'aggiornamento dei contenuti statici e dinamici di siti, portali e componenti web e mobile con contenuti testuali, grafici e multimediali; gestione dei contenuti di canali social e community on line.

TRATTAMENTO DEI DATI PERSONALI:

- Tipologia di dati che la piattaforma tratta: La piattaforma tratta dati pubblici.
- Tempo di conservazione dei dati: Il backup dei dati è conservato per 3 anni.
- Tempo di conservazione dei log di accesso o traffico: I log relativi ai firewall posti a protezione del sito, sono conservati per 12 mesi; i log relativi alla navigazione sul sito sono conservati per una settimana; il backup dei contenuti del sito sono conservati per 3 anni.
- Ulteriori misure tecniche di sicurezza applicate:

| Misura verticale | Descrizione |
|---|--|
| Profilazione | utilizzo di sistemi di profilazione con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di profilazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Utilizzo di sistemi di autenticazione multifattore | E' previsto l'uso di certificati digitali, PIN, o autenticazione per l'autenticazione dell'utente e/o per i servizi di cooperazione applicativa |
| Gestione del ciclo di vita delle credenziali (ex scadenza credenziali) | gestione del ciclo del provisioning delle credenziali di autenticazione e della profilazione, in particolare della |

| | |
|---|--|
| | scadenza della credenziale (anche in termini di gestione delle segnalazioni da sistemi centralizzati) |
| Tracciabilità accessi risorse (ex tracciabilità accessi DB e audit log applicativi) | possibilità di tracciare accessi alle risorse critiche (es DB, front end e back end del servizio, share di rete critici) |
| Audit log applicativi | nel DB è prevista la tracciatura dell'identificativo utente che ha inserito/modificato i dati delle tabelle e si è in grado di risalire a chi e quando ha inserito/modificato/cancellato il record |
| Abilitazioni puntuali accessi DB (proxy SQL) | utilizzo di proxy SQL |
| Minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento (ex scansione vulnerabilità) | (es politiche di aggiornamento del software, test funzionale e di vulnerabilità del software utilizzato, limitazioni dell'accesso fisico al materiale che contiene dati personali,) |
| Backup e restore | Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup |
| Business continuity/disaster recovery | esistenza di procedure per garantire la BC e/o il DR |

UTENTI ABILITATI AL SERVIZIO

Referenti operativi: con “referenti operativi” si indicano i committenti che possono beneficiare del servizio ovvero che sono autorizzati ad indicare modifiche ai siti web. Il referente operativi del sito web è il Responsabile della Direzione Sistemi Informativi.

MODALITÀ DI ACCESSO AL SERVIZIO

Il servizio viene attivato attraverso:

- richieste via e-mail inviate dai referenti del sito o da incaricati da essi autorizzati. Le richieste devono pervenire al seguente indirizzo di posta: helpweb@csi.it;
- attività pianificate ad inizio anno.

MODALITÀ DI EROGAZIONE DEL SERVIZIO

I servizi web, sia di front end sia di back end, sono disponibili via Internet H24 7 giorni su 7. L'orario di erogazione dei Servizi IT a supporto del Servizio Applicativo Comunicazione Digitale è il seguente:

| Servizio | Lunedì - Giovedì | Venerdì | Sabato - Domenica |
|----------------|--------------------------------|--------------------------------|-------------------|
| helpweb@csi.it | 09.00 - 12.30 13.30 - 17.00 | 09.00 - 12.30 13.30 - 16.00 | - |

9.3 SERVIZI DI PIATTAFORMA APPLICATIVI

9.3.1 CONTABILIA

Per la descrizione del servizio fare riferimento al documento “Catalogo e listino dei servizi del CSI”.

Preventivo economico:

| Servizi di piattaforma applicativi | Totale |
|------------------------------------|------------|
| Contabilia | € 5.500,00 |

TRATTAMENTO DEI DATI PERSONALI:

| | |
|---|--|
| Tipologia di dati che il servizio tratta | Dati di natura contabile, come gli stanziamenti dell’Ente, i documenti di spesa come le fatture e i pagamenti (mandati) e i documenti di entrata come i bollettini e gli incassi (reversali) e quindi una anagrafica dei soggetti (persone fisiche e giuridiche) coinvolti nei pagamenti e negli incassi (limitatamente alla Denominazione, Codice Fiscale o Partita Iva, Modalità di Pagamento del soggetto). Nei provvedimenti contabili possono essere richiamati gli estremi di atti amministrativi che potrebbero, in casi particolari riferirsi ad atti giudiziari o sanitari. |
| Tempo di conservazione dei dati | Durata necessaria al trattamento esplicitato nei registri dell'ente. Non utilizzabile come conservazione sostitutiva. |
| Tempo di conservazione dei log di accesso o traffico | 12 mesi |
| Profilazione | utilizzo di sistemi di profilazione con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di profilazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Autenticazione (ex autenticazione centralizzata) | utilizzo di sistemi di autenticazione (locali o nazionali) con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di autenticazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Utilizzo di sistemi di autenticazione multifattore | E previsto l'uso di certificati digitali, PIN, o autenticazione per l'autenticazione dell'utente e/o per i servizi di cooperazione applicativa |

| | |
|---|--|
| Gestione del ciclo di vita delle credenziali (ex scadenza credenziali) | gestione del ciclo del provisioning delle credenziali di autenticazione e della profilazione, in particolare della scadenza della credenziale (anche in termini di gestione delle segnalazioni da sistemi centralizzati) |
| Tracciabilità accessi risorse (ex tracciabilità accessi DB e audit log applicativi) | possibilità di tracciare accessi alle risorse critiche (es DB, front end e back end del servizio, share di rete critici) |
| Audit log applicativi | nel DB è prevista la tracciatura dell'identificativo utente che ha inserito/modificato i dati delle tabelle e si è in grado di risalire a chi e quando ha inserito/modificato/cancellato il record |
| Minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento (ex scansione vulnerabilità) | (es politiche di aggiornamento del software, test funzionale e di vulnerabilità del software utilizzato, limitazioni dell'accesso fisico al materiale che contiene dati personali,) |
| Cifratura del canale | Applicazione di canale cifrato per le comunicazioni mediante utilizzo di protocolli HTTPS e SSH |
| Backup e restore | Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup |

MODALITÀ DI ACCESSO AL SERVIZIO

Il servizio informatico è accessibile in modalità web all'indirizzo specificato di seguito.

| Servizio | Modalità di accesso |
|----------------------|---|
| Contabilia Dwbico | http://www.sistemapiemonte.it/cms/pa/tributi-finanza-e-bilancio |

La soluzione informatica proposta prevede l'erogazione dei servizi in rete via browser, sfruttando i vantaggi propri di quest'architettura: le postazioni di lavoro utente sono dotate di un browser, tramite il quale vengono effettuate tutte le operazioni previste dall'applicazione.

Non è quindi necessario procedere in loco all'installazione di alcun software specifico, in quanto i dati gestiti dall'applicazione risiedono centralmente.

UTENTI ABILITATI AL SERVIZIO

Utilizzatori del servizio sono tutte le risorse dell'Ente che, a vario titolo, sono coinvolte nella gestione contabile.

MODALITÀ DI EROGAZIONE DEL SERVIZIO

Le attività relative a Servizi IT sono svolte secondo l'orario di compresenza:

| Servizio | Lunedì - Giovedì | Venerdì | Sabato - Domenica |
|----------------------|--------------------------------|--------------------------------|-------------------|
| hd_contabilia@csi.it | 09.15 - 12.00 14.45 - 17.00 | 09.15 - 12.00 14.45 - 16.00 | - |

9.3.2 DEMATERIALIZZAZIONE

Per la descrizione del servizio fare riferimento al documento "Catalogo e listino dei servizi del CSI".

Preventivo economico:

| Servizi di piattaforma applicativi | Totale |
|------------------------------------|--------------------|
| Dematerializzazione | € 46.535,62 |
| TOTALE | € 46.535,62 |

Il servizio viene erogato a canone e prevede l'erogazione a 70 utenti registrati a sistema, uno spazio di disco 149 Gb con servizio ADVANCED e una previsione di 11.003 invii e ricezioni dalle caselle di PEC configurate su Doqui Acta.

TRATTAMENTO DEI DATI PERSONALI:

| | |
|---|--|
| Tipologia di dati che il servizio tratta | la piattaforma tratta documenti che possono contenere al loro interno dati personali o particolari. I dati strutturati gestiti nel database dalla piattaforma non prevedono esplicitamente campi specifici per i dati personali o particolari |
| Tempo di conservazione dei dati | la conservazione dei dati/documenti è stabilita da regolamenti e ulteriori policy definite dai singoli enti titolari degli stessi, in ottemperanza alle normative sulla gestione del protocollo informatico e sul mantenimento dei documenti amministrativi nell'archivio ufficiale. |
| Tempo di conservazione dei log di accesso o traffico | I log di accesso sono mantenuti per i tempi previsti dalle policy di sicurezza della server farm CSI a livello di sistemi infrastrutturali. La piattaforma applicativa non conserva log di accesso, ma registra solamente le modifiche ai dati/documenti in essa gestiti |
| Minimizzazione della quantità dei dati personali | rientrano misure di filtraggio e rimozione, riduzione della sensibilità attraverso la conversione, ridurre la natura identificativa del dato, ridurre l'accumulazione dei dati, limitare l'accesso ai dati |

| | |
|---|---|
| Profilazione | utilizzo di sistemi di profilazione con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di profilazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Autenticazione (ex autenticazione centralizzata) | utilizzo di sistemi di autenticazione (locali o nazionali) con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di autenticazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Utilizzo di sistemi di autenticazione multifattore | E previsto l'uso di certificati digitali, PIN, o autenticazione per l'autenticazione dell'utente e/o per i servizi di cooperazione applicativa |
| Gestione del ciclo di vita delle credenziali (ex scadenza credenziali) | gestione del ciclo del provisioning delle credenziali di autenticazione e della profilazione, in particolare della scadenza della credenziale (anche in termini di gestione delle segnalazioni da sistemi centralizzati) |
| Audit log applicativi | nel DB è prevista la tracciatura dell'identificativo utente che ha inserito/modificato i dati delle tabelle e si è in grado di risalire a chi e quando ha inserito/modificato/cancellato il record |
| Minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento (ex scansione vulnerabilità) | (es politiche di aggiornamento del software, test funzionale e di vulnerabilità del software utilizzato, limitazioni dell'accesso fisico al materiale che contiene dati personali,) |
| Cifratura del canale | Applicazione di canale cifrato per le comunicazioni mediante utilizzo di protocolli HTTPS e SSH |
| Backup e restore | Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup |
| Business continuity/disaster recovery | esistenza di procedure per garantire la BC e/o il DR |

UTENTI ABILITATI AL SERVIZIO

Utilizzatori del servizio sono tutte le risorse dell'Ente che, a vario titolo, sono coinvolte nella quotidiana gestione dei documenti e dei flussi documentali strutturati dell'Ente.

MODALITÀ DI ACCESSO AL SERVIZIO

Le componenti della piattaforma destinate all'utilizzo da parte degli utenti finali sono tipicamente erogate in modalità web e accedute via browser. Le url di pubblicazione del servizio sono esposte sulle apposite sezione

Intranet degli enti utilizzatori.

MODALITÀ DI EROGAZIONE DEL SERVIZIO

La gestione operativa osserva il seguente orario:

| Servizio | Lunedì - Giovedì | Venerdì | Sabato - Domenica |
|-----------------------|--------------------------------|--------------------------------|-------------------|
| assistenza.dwd@csi.it | 09.15 - 12.00 14.45 - 17.00 | 09.15 - 12.00 14.45 - 16.00 | - |

9.3.3 FATTURAZIONE ELETTRONICA

Per la descrizione del servizio fare riferimento al documento “Catalogo e listino dei servizi del CSI”, allegato alla Convenzione citata in premessa.

Preventivo economico:

| Servizi di piattaforma applicativi | Totale |
|------------------------------------|-----------------|
| Fatturazione Elettronica | € 669,60 |
| TOTALE | € 669,60 |

Il servizio a canone prevede l'erogazione del servizio per un numero stimato di 300 fatture.

TRATTAMENTO DEI DATI PERSONALI

| | |
|---|---|
| Tipologia di dati che il servizio tratta | Dati personali |
| Tempo di conservazione dei dati | 10 anni, durata necessaria al trattamento dello storico |
| Tempo di conservazione dei log di accesso o traffico | 24 mesi |
| Minimizzazione della quantità dei dati personali | rientrano misure di filtraggio e rimozione, riduzione della sensibilità attraverso la conversione, ridurre la natura identificativa del dato, ridurre l'accumulazione dei dati, limitare l'accesso ai dati |
| Profilazione | utilizzo di sistemi di profilazione con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di profilazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Autenticazione (ex autenticazione centralizzata) | utilizzo di sistemi di autenticazione (locali o nazionali) con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di autenticazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |

| | |
|---|--|
| Gestione del ciclo di vita delle credenziali (ex scadenza credenziali) | gestione del ciclo del provisioning delle credenziali di autenticazione e della profilazione, in particolare della scadenza della credenziale (anche in termini di gestione delle segnalazioni da sistemi centralizzati) |
| Tracciabilità accessi risorse (ex tracciabilità accessi DB e audit log applicativi) | possibilità di tracciare accessi alle risorse critiche (es DB, front end e back end del servizio, share di rete critici) |
| Minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento (ex scansione vulnerabilità) | (es politiche di aggiornamento del software, test funzionale e di vulnerabilità del software utilizzato, limitazioni dell'accesso fisico al materiale che contiene dati personali,) |
| Cifratura del canale | Applicazione di canale cifrato per le comunicazioni mediante utilizzo di protocolli HTTPS e SSH |
| Backup e restore | Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup |

UTENTI ABILITATI AL SERVIZIO

Il servizio è rivolto agli Enti della PA che debbano gestire fatture elettroniche.

MODALITÀ DI ACCESSO AL SERVIZIO

La soluzione proposta prevede l'erogazione dei servizi in modalità ASP, via browser, sfruttando i vantaggi propri di quest'architettura: le postazioni di lavoro utente sono dotate di un browser, tramite il quale vengono effettuate tutte le operazioni previste dalle applicazioni.

Non è quindi necessario procedere in loco all'installazione di alcun software specifico.

MODALITÀ DI EROGAZIONE DEL SERVIZIO

Il servizio di supporto è disponibile ai seguenti orari e contatti:

| Servizio | Lunedì - Giovedì | Venerdì | Sabato - Domenica |
|--|--------------------------------|--------------------------------|-------------------|
| Servizio di supporto hd_fatturaelettronica@csi.it | 09.15 - 12.00 14.45 - 17.00 | 09.15 - 12.00 14.45 - 16.00 | - |

9.3.4 PEC - POSTA ELETTRONICA CERTIFICATA

Per la descrizione del servizio fare riferimento al documento "Catalogo e listino dei servizi del CSI".

Preventivo economico:

| Servizi di piattaforma applicativi | Totale |
|------------------------------------|----------|
| Posta Elettronica Certificata | € 504,43 |

| | |
|---------------|-----------------|
| TOTALE | € 504,43 |
|---------------|-----------------|

Il servizio viene corrisposto attraverso un canone che include la messa a disposizione e la gestione operativa della piattaforma.

Vengono offerti i seguenti servizi:

- Casella PEC Articolata: 1 casella Standard e 1 casella Massiva;
- Assistenza standard (per 2 caselle);
- Assistenza evoluta (per 2 caselle).

DESCRIZIONE

La Posta Elettronica Certificata (PEC) è una tipologia particolare di [posta elettronica](#), disciplinata dalla legge italiana (la disciplina normativa è principalmente contenuta nel D.P.R. 11 febbraio 2005 n. 68 e nel decreto legislativo 7 marzo 2005 n. 82), che permette di dare a un messaggio di [posta elettronica](#) lo stesso valore legale di una [raccomandata](#) con avviso di ricevimento tradizionale garantendo così il non ripudio.

Il Consorzio, al fine di garantire una migliore operatività, offre ai committenti due tipologie di servizio di posta elettronica certificata: Semplice ed Articolata.

Il servizio di Posta Elettronica Certificata Semplice prevede un'unica tipologia di profilo (Casella PEC Semplice), con le seguenti caratteristiche:

- spazio di 1 GB, non incrementabile;
- durata di 1 anno;
- 200 invii al giorno (massimo).

Il dominio di posta disponibile è @cert.ruparpiemonte.it.

Il Consorzio ha la possibilità di gestire direttamente la configurazione del servizio, tramite interfaccia web con le seguenti funzionalità:

- autenticazione tramite user-id e password;
- creazione nuove caselle PEC;
- cancellazione caselle di PEC;
- reset password: nel caso in cui un utente abbia dimenticato la propria password, l'Amministratore del sistema ha la possibilità di eseguire il reset del campo password ad un valore impostato dall'Amministratore.

Il servizio di Posta Elettronica Certificata Articolata prevede molteplici tipologie (distinte in base alla dimensione delle caselle e dello spazio di archiviazione) ed opzioni (invio e gestione di messaggi in modalità massiva, personalizzazione del dominio); tutti i profili prevedono:

- possibilità di utilizzare un dominio generico @legalmail.it o personalizzato;
- possibilità di attivare filtro anti spam;
- possibilità di attivare notifica SMS per i nuovi messaggi certificati in casella;
- possibilità di attivare ricezione/rifiuto dei messaggi non PEC;
- integrazione con i più diffusi client di posta elettronica;

- completa aderenza alla normativa vigente;
- accesso e utilizzo della webmail attraverso canale sicuro;
- 4 possibili profili per le caselle.

Il servizio viene corrisposto attraverso un canone che include la messa a disposizione e la gestione operativa della piattaforma.

Il Consorzio offre inoltre un servizio di Assistenza Standard per tutte le tipologie di casella, oltre ad un servizio di Assistenza Evoluta per servizi aggiuntivi di integrazione e di troubleshooting per le sole caselle Articolate.

TRATTAMENTO DEI DATI PERSONALI:

- tipologia di dati che la piattaforma tratta: la piattaforma tratta dati anagrafici e codice fiscale degli utenti che accedono alle caselle di posta, e dati personali per quanto concerne il contenuto dei messaggi di posta elettronica
- tempo di conservazione dei log di accesso o traffico: i log relativi alle attività del server di posta sono conservati per 30 mesi
- tipologia di profilazione della piattaforma: la piattaforma non prevede privilegi differenti a secondo dell'utenza (ogni utente potrà vedere esclusivamente i contenuti delle eventuali caselle di cui possiede le credenziali)
- sicurezza del canale di comunicazione: in ottemperanza agli standard internazionali di crittografia, l'autenticazione, l'integrità dei dati, la confidenzialità nonché il trasporto sicuro dei dati durante la fruizione dei servizi della piattaforma è garantito dall'impiego dei protocolli TLS 1.x
- Durata della conservazione dei dati: la piattaforma mantiene il contenuto dei messaggi solo se essi sono presenti nella inbox di una casella attiva. Nel caso in cui una casella venga dismessa, non sarà più possibile utilizzarla per spedire o ricevere nuovi messaggi, e per i 30 giorni successivi alla dismissione l'utente potrà consultare i messaggi presenti in casella che siano pervenuti prima della revoca. Il contenuto della casella viene mantenuto per un periodo finito successivo alla dismissione (185 giorni nel caso di Posta Certificata Articolata, 30 giorni per la Posta Certificata Semplice) e il nome della medesima viene riservato (non potrà essere assegnato a diverso titolare): in questo periodo il titolare può eventualmente procedere al rinnovo della casella, ripristinandone le funzionalità e il contenuto. Trascorso tale termine, tutti i contenuti della casella verranno eliminati. Il nome della casella verrà riservato e non sarà più utilizzabile per nuove attivazioni.

SLA:

- DSPAPP - Tempo di disponibilità di una applicazione – L'indicatore misura la percentuale di disponibilità del servizio all'interno della finestra temporale di erogazione (H24 x 365 gg).
- APDEX - Application Performance Index - L'indicatore di servizi è denominato Apdex, Application Performance Index, ed ha come scopo quello di restituire un indice di soddisfazione delle aspettative dell'utente attraverso un modo uniforme di analizzare le misure ottenute dalla verifica dello stato attivo delle applicazioni monitorate.

UTENTI ABILITATI AL SERVIZIO

Servizio rivolto agli Enti Locali Consorziati sia direttamente che attraverso Ente sovraordinato (Provincia o Unione) al CSI Piemonte.

MODALITÀ DI ACCESSO AL SERVIZIO

Accesso e gestione tramite internet (webmail, che non richiede installazione sulla postazione di lavoro) e da client tradizionale (esempio Outlook o Thunderbird).

CANALI DI COMUNICAZIONE

Per le segnalazioni di malfunzionamento e le richieste di assistenza riguardanti i servizi di PEC, il Cliente dovrà utilizzare i canali mail o telefonici dell'hd generico di competenza per la propria tipologia di Ente (es. hd_comune@csi.it per il Comune di Torino, hd_agenzie@csi.it per AIPO, hd_entilocali@csi.it per i comuni, le province e le unioni di comuni...): il Contact Center di primo livello procederà ad aprire un ticket verso il gruppo di servizio corretto.

9.3.5 POSTA ELETTRONICA E SERVIZI DI COMUNICAZIONE UNIFICATA

Per la descrizione del servizio fare riferimento al documento “Catalogo e listino dei servizi del CSI”, allegato alla Convenzione citata in premessa.

Preventivo economico:

| Servizi di piattaforma applicativi | Totale |
|--|-------------------|
| Posta Elettronica e servizi di Comunicazione Unificata | € 4.634,40 |
| TOTALE | € 4.634,40 |

Vengono offerti i seguenti servizi:

- Profilo Base (25 caselle);
- Profilo Avanzato (63 caselle);
- Profilo Plus (25 caselle);
- Storage Aggiuntivo con replica (10 GigaByte);
- Storage Aggiuntivo con backup (200 GigaByte);
- Assistenza avanzata (per 113 caselle);
- Gestione credenziali di accesso (1 casella);
- Archivio posta on-line (300 GigaByte).

DESCRIZIONE:

Il Consorzio offre ai committenti un servizio di posta basato su piattaforma web (Unified Communication - UC), costituita da un portale di integrazione “Comunica”, ovvero un punto di

accesso unificato ai diversi servizi di comunicazione (tra cui posta elettronica, calendario, rubrica, messaggistica istantanea, audio e video chiamata), e da un portale di amministrazione dei servizi "PSNET".

Il sistema permette l'accessibilità dei servizi in mobilità (ovvero da qualsiasi PC dotato di browser e con una connessione internet) e la convergenza degli strumenti di comunicazione e collaborazione, fornendo agli utenti un unico punto di accesso per l'abilitazione, la gestione e l'utilizzo dei servizi disponibili.

Le funzionalità della Posta Elettronica prevedono:

- accesso e gestione della posta tramite internet (webmail, che non richiede installazione sulla postazione di lavoro) e da client tradizionale via IMAP (esempio Outlook o Thunderbird);
- accesso sicuro sia dall'interno (intranet) sia dall'esterno (internet) della rete dell'ente;
- possibilità di condivisione delle caselle di posta (di gruppo o personali) tra utenti;
- gestione scadenza password secondo i vincoli di legge;
- console di gestione degli account di posta (portale di amministrazione dei servizi – PSNET);
- servizio di AntiSpam e AntiVirus centralizzato;
- servizio di Instant Messaging (Chat);
- gestione degli alias in ingresso;
- gestione dei filtri di ricezione;
- rilascio o aggiornamento della credenziale per accesso come amministratore al portale di amministrazione (PSNET);
- parametri di configurazione per l'accesso ai servizi;
- manuale d'uso di Comunica e delle funzioni di amministrazione/configurazione di base su PSNET;
- Backup messaggi di posta secondo le seguenti modalità:
 - backup dei messaggi di posta elettronica secondo modalità incrementale (giornaliera e conservato per tre settimane, settimanale conservato per tre mesi, mensile conservata per un anno e annuale conservato per 3 anni);
 - backup giornaliero, secondo la normativa di riferimento, dei tracciati log relativi al transito di tutti i messaggi ricevuti ed inviati. I backup dei log sono garantiti per 12 mesi;
- Ripristino messaggi di posta:
 - email cancellate entro i 30 giorni: nel caso in cui l'utente effettui la rimozione di un contenuto (anche dal cestino), è possibile ripristinare i messaggi cancellati negli ultimi 30 giorni direttamente nella inbox dell'utente.
 - email cancellate oltre i 30 giorni: le email cancellate da più di 30 giorni possono essere ripristinate tramite procedura assistita di recupero a partire da una copia disponibile di salvataggio (backup).

Si precisa che la configurazione via client (su pc o dispositivo mobile) della casella garantisce la corretta sincronizzazione dei messaggi di posta per ciascun profilo di casella indicato nel seguito, ma non dei calendari e delle rubriche.

Il servizio è proposto in tre profili distinti in base alla dimensione delle caselle e alla disponibilità di calendario e rubrica eventualmente fruibili in mobilità.

Profilo Base

- dimensione casella: 500 MB

Profilo Avanzato

- dimensione casella: 1 GB
- disponibilità di un calendario personale e condiviso
- gestione account di posta multipli
- disponibilità di attivazione del servizio INFOSTORE ovvero la possibilità di disporre di uno spazio disco accessibile tramite web per la condivisione di documenti, a slot di 10 GB

Profilo Plus

- dimensione casella: 1 GB
- disponibilità di un calendario personale e condiviso
- gestione account di posta multipli
- disponibilità di attivazione del servizio INFOSTORE ovvero la possibilità di disporre di uno spazio disco accessibile tramite web per la condivisione di documenti, a slot di 10 GB
- sincronizzazione di calendario e rubrica personale con dispositivi mobili¹.

In aggiunta a quanto indicato nel Servizio Standard, se richiesto, è possibile attivare servizi aggiuntivi quali:

- **Storage aggiuntivo con backup:** ampliamento della casella rispetto alla dimensione standard del profilo. Il backup dello storage aggiuntivo avviene secondo le stesse modalità del servizio Base.
- **Storage aggiuntivo con replica:** qualora non si ritenesse necessario il mantenimento incrementale dei backup, è possibile richiedere la gestione delle caselle mediante la sola replica dei dati. In tal caso, si potranno recuperare le mail cancellate esclusivamente entro 30 giorni.
- **Gestione credenziali di Accesso:** servizio opzionale di creazione e gestione delle credenziali e dei profili degli utenti da parte del CSI.
- **Assistenza Avanzata:** comprende le attività di verifica sui rapporti di consegna dei messaggi di posta o di troubleshooting in caso di mancato recapito, la fornitura dei manuali operativi per la configurazione di client di posta (Microsoft Outlook, Mozilla Thunderbird, ecc.) per pc e dispositivi mobili, il supporto in merito alle funzionalità di UC per integrazione con sistemi di interscambio documentale e la modifica delle deleghe sulle caselle di gruppo in sostituzione dell'amministratore.

¹ All'atto della stesura del presente catalogo sono supportati i seguenti sistemi operativi: Android 4 e versioni successive, Windows Phone 7, Windows Phone 8, iOS 7, iOS 8, iOS 9.

- **Archiviazione posta on-line:** il servizio può essere attivato per tutte le caselle dell'Ente o per un suo sottoinsieme. Le funzioni di archiviazione/ricerca e consultazione dei messaggi archiviati sono gestite in autonomia dal singolo utente direttamente tramite l'interfaccia del sistema. Il dimensionamento dello spazio di archivio è configurato a livello di ente. Il servizio viene corrisposto attraverso un Canone che include la messa a disposizione e la gestione operativa della piattaforma e il Customer Service Desk.

Tutte le configurazioni, le regole di avvio ed i servizi aggiuntivi della soluzione di posta elettronica dovranno essere concordati con l'Ente, che dovrà indicare a CSI un referente interno di servizio. Quest'ultimo sarà avvisato in caso di fermi di servizio programmati o straordinari, nuove release, etc.

Queste attività, nonché le attività di migrazione ed avvio, sono oggetto di specifica offerta economica di start-up.

TRATTAMENTO DEI DATI PERSONALI:

- tipologia di dati che la piattaforma tratta: la piattaforma tratta dati anagrafici e codice fiscale degli utenti che accedono alle caselle di posta, e dati personali per quanto concerne il contenuto dei messaggi di posta elettronica
- tempo di conservazione dei log di accesso o traffico: i log relativi alle attività del server di posta sono conservati per 12 mesi
- tipologia di profilazione della piattaforma: il front-end della piattaforma non prevede privilegi differenti a secondo dell'utenza (ogni utente potrà vedere esclusivamente i contenuti della propria casella individuale e delle eventuali caselle condivise su cui sia stato delegato); l'interfaccia di amministrazione prevede invece una figura di amministratore che ha a disposizione tutti i privilegi per creare, rimuovere caselle e modificarne le risorse ed i permessi, mentre l'accesso come utente consente di utilizzare un sottoinsieme di funzionalità (ad esempio il reset della password)
- sicurezza del canale di comunicazione: in ottemperanza agli standard internazionali di crittografia, l'autenticazione, l'integrità dei dati, la confidenzialità nonché il trasporto sicuro dei dati durante la fruizione dei servizi della piattaforma è garantito dall'impiego dei protocolli TLS 1.x
- Durata della conservazione dei dati: il backup dei messaggi (effettuato secondo modalità incrementale come precedentemente indicato) è conservato per un massimo di 3 anni. Nel caso in cui il Cliente ritenga opportuno che venga effettuata una conservazione con tempistiche superiori dovrà presentare esplicita richiesta formale.

SLA:

- DSPAPP - Tempo di disponibilità di una applicazione – L'indicatore misura la percentuale di disponibilità del servizio all'interno della finestra temporale di erogazione (H24 x 365 gg).
- APDEX - Application Performance Index - L'indicatore di servizi è denominato Apdex, Application Performance Index, ed ha come scopo quello di restituire un indice di soddisfazione delle aspettative dell'utente attraverso un modo uniforme di analizzare le misure ottenute dalla verifica dello stato attivo delle applicazioni monitorate.

UTENTI ABILITATI AL SERVIZIO

Servizio rivolto agli Enti Locali Consorziati sia direttamente che attraverso Ente sovraordinato (Provincia o Unione) al CSI Piemonte.

MODALITÀ DI ACCESSO AL SERVIZIO

Accesso e gestione tramite internet (webmail, che non richiede installazione sulla postazione di lavoro) e da client tradizionale (esempio Outlook o Thunderbird).

CANALI DI COMUNICAZIONE

Per le segnalazioni di malfunzionamento e le richieste di assistenza riguardanti i servizi di posta elettronica, il Cliente dovrà utilizzare i canali mail o telefonici dell'hd generico di competenza per la propria tipologia di Ente (es. hd_comune@csi.it per il Comune di Torino, hd_agenzie@csi.it per AIPO, hd_entilocali@csi.it per i comuni, le province e le unioni di comuni...): il Contact Center di primo livello procederà ad aprire un ticket verso il gruppo di servizio corretto.

9.3.6 SERVIZI AL PERSONALE

Per la descrizione del servizio fare riferimento al documento “Catalogo e listino dei servizi del CSI”, allegato alla Convenzione citata in premessa.

Preventivo economico:

| Servizi di piattaforma applicativi | Totale |
|------------------------------------|-------------------|
| Servizi al Personale | € 3.792,12 |
| TOTALE | € 3.792,12 |

L’offerta prevede l’erogazione dei seguenti servizi:

| | |
|--|---|
| <ul style="list-style-type: none"> • Servizio Base contabilità economica; • Servizio Rap base plus (servizio base comprensivo di due moduli opzionali a scelta); • Servizio base gestione giuridica; • DWH Cedolini; | per un volume preventivato di 759 cedolini elaborati. |
| <ul style="list-style-type: none"> • Rimissioni delle credenziali. | per un volume preventivato di 1 credenziali. |

TRATTAMENTO DEI DATI PERSONALI:

| | |
|---|---|
| Tipologia di dati che il servizio tratta | Dati anagrafici dei soggetti a cui vengono rilasciate le credenziali |
| Tempo di conservazione dei dati | i dati utente non vengono mai cancellati a meno di specifica richiesta dell’utente medesimo |
| Tempo di conservazione dei log di accesso o traffico | 36 mesi |
| Sicurezza del canale di comunicazione | HTTPS |
| Ulteriori misure tecniche di sicurezza applicate | La piattaforma prevede la criptazione dei dati |

| | |
|---|--|
| Profilazione | utilizzo di sistemi di profilazione con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di profilazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Utilizzo di sistemi di autenticazione multifattore | E previsto l'uso di certificati digitali, PIN, o autenticazione per l'autenticazione dell'utente e/o per i servizi di cooperazione applicativa |
| Audit log applicativi | nel DB è prevista la tracciatura dell'identificativo utente che ha inserito/modificato i dati delle tabelle e si è in grado di risalire a chi e quando ha inserito/modificato/cancellato il record |
| Cifratura del dato | mezzi implementati per assicurare la confidenzialità dei dati archiviati (in database, file, backup etc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di compromissione etc.) |
| Cifratura del canale | Applicazione di canale cifrato per le comunicazioni mediante utilizzo di protocolli HTTPS e SSH |
| Backup cifrati | utilizzo di sistemi per la cifratura dei backup |

UTENTI ABILITATI AL SERVIZIO

Referenti Master

MODALITÀ DI ACCESSO

I contatti potranno essere:

- telefonici ai numeri appositamente comunicati ai referenti:
- dal Lunedì al Venerdì dalle ore 9.00 alle ore 12.30
- via fax al n. 011.316.84.96 o e-mail agli indirizzi comunicati ai referenti dell'Ente.

Le richieste pervenute via fax o e-mail saranno prese in carico nel più breve tempo possibile e, comunque, entro i termini di utili alla corretta erogazione del servizio.

Il Servizio include la possibilità di accedere e consultare un apposito Portale informativo sulle novità e sulle modalità di fruizione del servizio, dedicato agli Uffici interessati. Il Portale è raggiungibile al seguente indirizzo: "<http://servizipersonale.sistemapiemonte.it/cms/>".

MODALITÀ DI EROGAZIONE

I servizi sono erogati sulla base delle funzionalità previste in ciascun applicativo, delle modalità e tempi indicati nel calendario operativo annuo e, ove previsti, dei calendari e delle note operative emesse in funzione della produzione dei servizi periodici.

L'erogazione dei servizi che richiedono l'avviamento sarà effettuata a conclusione delle attività di avviamento e addestramento all'uso, con le modalità e le tempistiche concordate tra Consorzio ed Ente.

In particolare per i Servizi di Contabilità Economica e Convenzioni Nazionali Uniche il servizio si svolge seguendo il calendario operativo predisposto annualmente. Esso definisce, per ciascun mese, le date di scadenza per l'immissione dei dati, per l'elaborazione e la pubblicazione dei cedolini e dei relativi output e per la storicizzazione delle risultanze mensili del calcolo (consolidamento cedolino nel calendario operativo). I calendari sono predisposti al fine di recepire il maggior numero di eventi economici che incidono sull'elaborazione del mese di elaborazione. Nel periodo di tempo che intercorre tra elaborazione dei cedolini e la loro storicizzazione i dati sono disponibili "on-line" in sola lettura per le ulteriori operazioni di controllo.

I calendari e le note informative, che regolano le modalità di erogazione dei servizi, sono pubblicati nelle apposite sezioni del Portale dei Servizi al Personale.

Le eventuali richieste di aggiornamenti e/o modifiche sul DB, non conseguenti ad anomalie del sistema, devono pervenire all'assistenza prima dei 5 gg antecedenti la chiusura del mese o del servizio. Eventuali richieste pervenute oltre tale data saranno oggetto di eventuale valutazione di fattibilità e/o di impegno economico.

9.3.7 SITO WEB

Per la descrizione del servizio fare riferimento al documento "Catalogo e listino dei servizi del CSI", allegato alla Convenzione citata in premessa.

Preventivo economico:

| Servizi di piattaforma applicativi | Totale |
|------------------------------------|-------------------|
| Siti Web | € 2.940,00 |
| TOTALE | € 2.940,00 |

Vengono offerti i servizi relativamente ad 1 sito web.

DESCRIZIONE

Il servizio Sito web consiste nella progettazione, realizzazione e gestione di un sito web attraverso uno strumento open source di Content Management System (CMS).

Il servizio si riferisce a siti web standard e di complessità medio-bassa, sia in termini di tipologia di contenuti sia di numero di livelli informativi.

Il sito rappresenta uno strumento di comunicazione digitale, fruibile da tutti i target dell'Ente committente, attraverso un'interfaccia gradevole, dinamica e flessibile.

Il sito realizzato avrà le seguenti caratteristiche:

- usabile e accessibile, in linea con la normativa italiana sull'accessibilità;
- coerente con le Linee guida di design dei siti della P.A. di AgID, con l'obiettivo di rendere

l'accesso alle informazioni semplice, rapido e chiaro;

- responsive, ossia fruibile da qualsiasi dispositivo anche in mobilità;
- ottimizzato per i principali motori di ricerca;
- abilitato al monitoraggio delle attività degli utenti (*analytics*);
- dotato di un back-end per la gestione dei contenuti autonoma e in sicurezza da parte dell'Ente.

Il servizio proposto prevede:

Canone: è annuale e comprende tutte le attività volte ad assicurare il corretto e continuativo funzionamento del sito web: la "Gestione Operativa Applicazione", la "Manutenzione Correttiva", la "Manutenzione Perfettiva". Inoltre sono comprese le attività seguenti:

- Aggiornamento piattaforma CMS: aggiornamenti di "minor release" della piattaforma CMS con cui sono realizzati i siti.
- Gestione profilazione: comprende le attività utili al corretto accesso al back-office dei CMS: richieste di abilitazione di un utente ad un back-office. reset della password, disabilitazione ai back-office, modifica della profilazione, gestione dei malfunzionamenti legati all'accesso al back-office del CMS.
- Sicurezza: monitoraggio della quantità e tipologia di traffico sul sito tramite appositi strumenti. Monitoraggio delle community dei CMS OpenSource per essere sempre informati su eventuali problemi di sicurezza. Aggiornamenti delle piattaforme con nuove versioni e/o installazione di eventuali patch di sicurezza;
- Nuove componenti: attività di scouting per individuare nuove componenti delle piattaforme CMS utili per le attività di aggiornamento / pubblicazione contenuti. Test, installazione e formazione sulle componenti individuate.
- Accessibilità: periodici test sui contenuti pubblicati per verificarne il grado di accessibilità. I risultati vengono raccolti in report che vengono forniti e discussi con il Cliente;
- Adeguamento alla normativa: costante attenzione all'evoluzione della normativa sulla pubblicazione dei contenuti web e ai relativi obblighi di legge, con attenzione sulle regole per l'accessibilità, l'usabilità e sull'evoluzione delle linee guida dell'Autorità centrale per la pubblicazione e la fruizione di contenuti web;
- Analytics: attività di analisi degli accessi ai siti attraverso strumenti di web analytics (GoogleAnalytics, Piwik,); produzione report e statistiche descrittive relative agli accessi al sito.

TRATTAMENTO DEI DATI PERSONALI:

- tipologia di dati che la piattaforma tratta: La piattaforma tratta dati pubblici.
- tempo di conservazione dei log di accesso o traffico: secondo indicazioni del DPO dell'Ente
- sicurezza del canale di comunicazione: http / https
- **TRATTAMENTO DEI DATI PERSONALI:**

| Misura verticale | Descrizione |
|------------------|-------------|
|------------------|-------------|

| | |
|---|--|
| Minimizzazione della quantità dei dati personali | rientrano misure di filtraggio e rimozione, riduzione della sensibilità attraverso la conversione, ridurre la natura identificativa del dato, ridurre l'accumulazione dei dati, limitare l'accesso ai dati |
| Backup e restore | Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup |
| Business continuity/disaster recovery | esistenza di procedure per garantire la BC e/o il DR |

UTENTI ABILITATI AL SERVIZIO

Dipendenti dell'Ente.

MODALITÀ DI ACCESSO

Via e-mail o chiamata telefonica.

MODALITÀ DI EROGAZIONE

L'accesso al servizio per assistenza e supporto è il seguente:

| Servizio | Lunedì - Giovedì | Venerdì | Sabato - Domenica |
|------------------------------------|------------------|---------------|-------------------|
| helpweb@csi.it Tel. 011 3169666 | 09.00 - 17.00 | 09.00 - 16.00 | - |

9.3.8 TELEMACO

Per la descrizione del servizio fare riferimento al documento "Catalogo e listino dei servizi del CSI",

Preventivo economico:

| Servizi di piattaforma applicativi | Totale |
|------------------------------------|-------------------|
| Telemaco | € 1.403,50 |
| TOTALE | € 1.403,50 |

L'offerta prevede l'erogazione dei seguenti servizi:

- Quota fissa fino a 250 consultazioni (1 fornitura);
- Singola consultazione aggiuntiva oltre le 250 (sono state previste 1.100 consultazioni oltre le 250).

DESCRIZIONE DEI SERVIZI IT EROGATI

Il servizio Telemaco consente la consultazione, tramite chiavi di accesso, dei dati ufficiali del Registro Imprese di Infocamere. Il Registro Imprese può essere definito come l'anagrafe delle imprese: vi si trovano infatti i dati (costituzione, modifica, cessazione) di tutte le imprese con qualsiasi forma giuridica e settore di attività economica, con sede o unità locali sul territorio nazionale, nonché gli altri soggetti previsti dalla legge. Il servizio consente di ricercare le principali informazioni relative

alle imprese quali denominazione, statuto, amministratori, sede, altro e tutte le eventuali variazioni comunicate al Registro dopo l'iscrizione.

Sono a disposizione degli utenti funzioni per il monitoraggio delle consultazioni effettuate e fatturabili.

Il servizio viene corrisposto attraverso un Canone che include il Customer Service Desk.

Vincoli e responsabilità

- L'ente si impegna ad assicurare che i dati camerali a cui hanno accesso saranno utilizzati esclusivamente per lo svolgimento delle normali attività relative alle procedure interne dei propri uffici, con divieto assoluto di fornirli a terzi anche a titolo gratuito.
- È vietato pertanto, qualsiasi atto di commercio dei dati camerali accessibili tramite Telemaco.
- È vietata la riproduzione dei dati su supporti elettronici o similari.
- L'inosservanza di tali disposizioni costituisce grave inadempimento da parte dell'Amministrazione e darà facoltà a CSI Piemonte ed InfoCamere di procedere all'immediata interruzione del servizio ed alla risoluzione del presente contratto ai sensi dell'art.1456 del codice civile, con riserva di chiedere il risarcimento dei danni subiti.

Compatibilità e prerequisiti Hw / Sw

Per poter fruire del servizio deve essere attivo un collegamento ad internet. Non sono necessari altri requisiti HW/SW.

Perimetro del servizio

Il CSI Piemonte fornisce le chiavi di accesso al servizio, che viene fornito attraverso un collegamento fisico proprietario al centro di calcolo InfoCamere di Padova utilizzando la rete Internet. Il servizio viene conteggiato a consumo rispetto alle transazioni effettuate nel corso di validità della presente proposta economica.

TRATTAMENTO DEI DATI PERSONALI:

- Tipologia di dati che la piattaforma tratta: dati personali.
- Tempo di conservazione dei log di accesso o traffico: non è prevista la conservazione dei log.
- Tipologia di profilazione della piattaforma: profilo in lettura come gestore delle chiavi assegnate al CSI.
- Sicurezza del canale di comunicazione: HTTPS.
- Durata della conservazione dei dati: 10 anni.
- Quali misure di sicurezza sono applicate ai dati personali e particolari (ovvero se la piattaforma applica la cifratura di dati oppure la pseudonimizzazione): non è prevista cifratura o pseudonimizzazione.

UTENTI ABILITATI AL SERVIZIO

Gli utenti abilitati sono gli intestatari delle chiavi di accesso Telemaco.

MODALITÀ DI ACCESSO

L'accesso al servizio viene indicato al diretto utilizzatore nella comunicazione di attivazione inviata.

MODALITÀ DI EROGAZIONE

La disponibilità dei servizi InfoCamere è stabilita dal produttore stesso come di seguito indicato: dal lunedì al sabato dalle ore 8.00 alle ore 21.00 (ad esclusione delle festività infrasettimanali). In caso di malfunzionamenti o non disponibilità del servizio, InfoCamere mette a disposizione un servizio di help-desk. Il servizio di help desk non fornisce assistenza in merito a malfunzionamenti delle apparecchiature hardware utilizzate per accedere al Servizio, e in merito al software installato

9.4 SERVIZI DI PIATTAFORMA INFRASTRUTTURALI

9.4.1 SERVIZI VIRTUAL DATA CENTER

Preventivo economico:

| Servizi di piattaforma infrastrutturali | Totale |
|---|--------------------|
| Virtual data center | € 37.337,77 |
| TOTALE | € 37.337,77 |

DESCRIZIONE:

Il CSI mette a disposizione dei committenti servizi di “Private Cloud” erogati su infrastrutture dislocate nei Datacenter di Torino e Vercelli. I servizi Cloud includono il Customer Service Desk e si articolano in:

- IaaS (Infrastructure as a Service) è un modello di servizio che fornisce l'accesso a una risorsa informatica, specificatamente un hardware virtualizzato cioè un'infrastruttura di elaborazione appartenente a un ambiente virtualizzato, il "Cloud", tramite una connessione; sono disponibili varie tipologie di Virtual Private Cloud, Virtual Machine, Virtual Network, Backup as a Service;
- PaaS e DBaaS Gestiti: Platform as a Service e Data Base as a Service sono servizi che forniscono agli sviluppatori una piattaforma e un ambiente (PAAS) oppure un Data Base (DBAAS) per costruire applicazioni e servizi su Internet; gli ambienti disponibili comprendono: MySQL versione commerciale, PostgreSQL versione commerciale, MsSql, Oracle Enterprise Edition, Jboss versione commerciale, Tomcat versione Community, servizi di condivisione File, servizi di supporto Cloud ecosistema federato CSI, tecnologie di cooperazione (WSO2); comprende il backup.

Perimetro di attività (incluse/non incluse)

Attività incluse nel servizio:

- Creazione Organization Unit;
- Assegnazione risorse elaborative e storage al VDC;
- Configurazione connettività di rete;
- Configurazione minima di sicurezza sui vShield Edge Gateway per consentire la raggiungibilità dei servizi dedicati al VDC erogati dal CSI-Piemonte (KMS, Proxy, Mail Server per invio mail applicative, DNS);
- Messa a disposizione del catalogo contenente immagini con i principali sistemi operativi Linux / Windows pre-installati;
- Messa a disposizione servizio proxy in uscita da rete Rugar;
- Messa a disposizione server KMS per attivazione licenze Microsoft;
- Messa a disposizione mail server per invio di posta applicativa in modalità sicura e autenticata con eventuale creazione di un account;
- Messa a disposizione due server DNS gestiti da CSI-Piemonte;
- Possibilità di attivazione opzione di backup degli ambienti virtuali attestati sul VDC e restore

in self-service con tecnologia Veeam Backup & Restore;

Attività non incluse nel servizio:

- Gestione sistemistica delle vApp;
- Gestione della sicurezza del VDC.

Informazioni minime per l'attivazione

- Numero di CPU;
- GB di RAM;
- GB di Storage;
- Numero IP RUPAR e tipologia di vShield Edge;
- Numero IP Internet e tipologia di vShield Edge;
- Esigenza di attivazione opzione di Backup Veeam;
- Esigenza di account per invio autenticato mail applicativa.

Up-time garantito

99,9%

Tempi di consegna

3gg

TRATTAMENTO DEI DATI PERSONALI:

| | |
|--|---|
| Profilazione | utilizzo di sistemi di profilazione con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di profilazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Autenticazione (ex autenticazione centralizzata) | utilizzo di sistemi di autenticazione (locali o nazionali) con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di autenticazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Gestione del ciclo di vita delle credenziali (ex scadenza credenziali) | gestione del ciclo del provisioning delle credenziali di autenticazione e della profilazione, in particolare della scadenza della credenziale (anche in termini di gestione delle segnalazioni da sistemi centralizzati) |
| Tracciabilità accessi risorse (ex tracciabilità accessi DB e audit log applicativi) | possibilità di tracciare accessi alle risorse critiche (es DB, front end e back end del servizio, share di rete critici) |
| Audit log applicativi | nel DB è prevista la tracciatura dell'identificativo utente che ha inserito/modificato i dati delle tabelle e si è in grado di risalire a chi e quando ha inserito/modificato/cancellato il record |

| | |
|---|--|
| Abilitazioni puntuali accessi DB (proxy SQL) | utilizzo di proxy SQL |
| Minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento (ex scansione vulnerabilità) | (es politiche di aggiornamento del software, test funzionale e di vulnerabilità del software utilizzato, limitazioni dell'accesso fisico al materiale che contiene dati personali,) |
| Cifratura del dato | mezzi implementati per assicurare la confidenzialità dei dati archiviati (in database, file, backup etc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di compromissione etc.) |
| Cifratura del canale | Applicazione di canale cifrato per le comunicazioni mediante utilizzo di protocolli HTTPS e SSH |
| Backup e restore | Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup |
| Backup cifrati | utilizzo di sistemi per la cifratura dei backup |
| Business continuity/disaster recovery | esistenza di procedure per garantire la BC e/o il DR |

MODALITÀ DI ACCESSO AL SERVIZIO

N.A.

CANALI DI COMUNICAZIONE

L'accesso al servizio per le richieste di assistenza è disponibile utilizzando il seguente indirizzo di posta elettronica: hd_regione@csi.it

9.4.1.1.1 Servizio Storage as a Service**Descrizione del contesto tecnologico di riferimento**

La messa a disposizione dei servizi di storage avviene su infrastrutture ridondate e configurate in alta affidabilità. La principale caratteristica di tale configurazione prevede che in caso di fault di una componente di front-end o back-end degli apparati, intervengono meccanismi di ridondanza che permettono di ottenere l'erogazione continua del servizio. In caso, invece, di rottura di un disco, intervengono meccanismi di protezione tipici della configurazione hardware RAID, La configurazione RAID con dischi "hot spare" consente in caso di guasto di un disco, la messa in fault dello stesso e la sua sostituzione con un altro disco prelevato dal gruppo di dischi definiti "hot spare".

È attivo inoltre un sistema di monitoraggio chiamato "call home" che in tempo reale invia al centro di supporto dei fornitori tutte le segnalazioni di anomalia/avarie che possono intervenire durante il normale funzionamento degli apparati.

Perimetro di attività (incluse/non incluse)

Attività incluse:

- Analisi richiesta;
- Definizione tipologia in funzione dei requisiti (IOPS);
- Assegnazione spazio disco agli ambienti applicativi;
- Backup con snapshot e/o replica del dato

Informazioni minime per l'attivazione

- Descrizione del servizio che utilizzerà lo storage richiesto;
- Quale è l'uso per cui è richiesto;
 - Immagazzinamento dei dati di backup;
 - Indici e backup dei DB;
 - File server;
 - Applicativo;
 - Archivi storici, statici, dinamici;
 - Volumi in replica;
- Indicare se il dato è statico o dinamico;
- Dimensionamento in GB dello spazio richiesto.

Up-time garantito

99,5%

Tempi di consegna

5gg

Metrica

GB

Modalità di erogazione del servizio

Nell'ambito dell'area Sistemi e Reti, il gruppo Sistemisti-Unix si occupa di:

- Assegnare lo spazio storage adatto al volume da creare (midrange/lowrange);
- Creare lato NAS l'aggregato delle LUN esposte dallo storage;
- Creare sull'aggregato i volumi che saranno accessibili tramite protocolli NFS o CIFS;
- Associare il volume ad un filer.

Il servizio di storage NAS è erogato H24

| Servizio | Lunedì - Venerdì | Sabato - Domenica |
|--|------------------|-------------------|
| Richiesta per il servizio di storage NAS | 09.00 – 17.00 | - |

9.4.1.1.2 Gestione sistemistica server Cloud

Descrizione del servizio

Il servizio di gestione sistemistica server Cloud prevede l'erogazione della gestione delle vApp Linux e Windows installate sul il Cloud del CSI-Piemonte.

Il servizio di gestione sistemistica server Cloud prevede l'esecuzione di attività di installazione e configurazione delle componenti del sistema operativo della vApp a cui si applica il servizio. Le attività sono concordate preventivamente da un lato con il cliente, con il tramite delle strutture aziendali preposte al dialogo con gli Enti, e dall'altro con gli eventuali fornitori terzi.

Di seguito vengono elencati i principali compiti dei sistemisti della Direzione Datacenter nello svolgimento del servizio:

L'aggiornamento del sistema operativo e dei software di base locali installati sui server;

L'installazione delle patch e degli aggiornamenti di sicurezza proposti da DPO, nell'ambito della versione e della release del sistema operativo installato;

Identificazione degli impatti e la ricerca della loro causa, attraverso un processo correttivo (troubleshooting), a fronte del presentarsi di malfunzionamenti legati ai sistemi operativi installati;

La gestione e l'aggiornamento del sistema locale antivirus dei server ai quali il servizio è applicato.

Nello svolgimento delle attività di gestione quotidiana, i sistemisti curano il mantenimento del controllo degli accessi finalizzato a proteggere e limitare gli interventi sui server solo agli utenti autorizzati, in accordo con le indicazioni fornite dall'Ente. Sono previste azioni giornaliere eseguite a bordo dei server oggetto del servizio di gestione sistemistica server Cloud, il cui fine è quello di garantire una buona e costante erogazione del servizio, una corretta manutenzione, un monitoraggio delle risorse così da prevenire disservizi.

I sistemisti procedono nel quotidiano alla gestione delle utenze di dominio Active Directory e LDAP, e dei relativi livelli di autorizzazione attribuendole, ai gruppi definiti.

Inoltre, al fine di ridurre la superficie di attacco del sistema operativo delle vApp i sistemisti procedono alla costante messa in sicurezza del sistema attraverso l'applicazione delle best-practice relative all'Hardening dei sistemi, con l'eventuale rimozione o disabilitazione di software, di utenze o di servizi non necessari.

Al fine di verificare e configurare le impostazioni relative a computer e utenti nelle reti basate su servizi di dominio Active Directory, i sistemisti operano attraverso l'utilizzo di group policy di dominio, strumento attraverso cui è possibile creare politiche personalizzate per gli utenti e i computer; le group policy consentono di definire e distribuire le configurazioni a numerosi server in modo centralizzato con una singola operazione.

Nell'ambito del servizio vengono inoltre gestiti i servizi di rete Microsoft, quali i servizi DNS e WINS, connessi alle funzionalità del dominio Active Directory.

Nell'ambito della predisposizione della struttura dello spazio disco utente, i sistemisti creano e gestiscono le home directory, escluse altre profilazioni legate a servizi di File server.

Qualora il server a cui si applica il servizio di gestione sistemistica server Cloud sia sottoposta a backup, i sistemisti si occupano dell'esecuzione e della verifica della corretta esecuzione delle procedure di backup/restore.

Attivazione di procedure di backup e monitoraggio giornaliero tramite l'analisi di file di log. Su puntuale richiesta del cliente, i sistemisti attivano le opportune procedure di restore dei file.

L'ottimizzazione dei sistemi è un'attività che viene effettuata al termine dell'installazione fisica e logica dei sistemi. Il fine è quello di ottimizzare le prestazioni di sistema, bilanciando le risorse hardware, adeguando le aree storage e parametrizzando il software di base. L'attività in molti casi prosegue con la fase di collaudo dei sistemi e una eventuale messa a punto.

Perimetro tecnologico gestito

I sistemisti della Direzione Datacenter dispongono di competenze tecniche specifiche per gestire i sistemi operativi di seguito elencati. Le versioni dei Sistemi operativi sono vincolate dall'essere supportati dal produttore e compatibili con le infrastrutture hardware del CSI-Piemonte.

Ambito Windows

Di seguito l'elenco dei sistemi operativi Microsoft installati a bordo di vApp:

- Microsoft Windows 2000 Advanced Server;
- Microsoft Windows 2000 Professional;
- Microsoft Windows 2000 Server;
- Microsoft Windows NT 4.0 Server;
- Microsoft Windows Server 2003 Enterprise Edition;
- Microsoft Windows Server 2003 R2 Standard Edition;
- Microsoft Windows Server 2003 R2 Standard x64 Edition;
- Microsoft Windows Server 2003 Standard Edition;
- Microsoft Windows Server 2003 Web Edition;
- Microsoft Windows Server 2008 Standard;
- Microsoft Windows Server 2008 R2 Enterprise;
- Microsoft Windows Server 2008 R2 Standard;
- Microsoft Windows Server 2008 Standard Edition;
- Microsoft Windows Server 2012 R2 Standard;
- Microsoft Windows Server 2012 Standard;
- Microsoft Windows Server 2012 Standard Edition.

Ambito Linux/Unix

Di seguito l'elenco dei sistemi operativi Linux/Unix installati a bordo di server virtuali:

- Centos 4/5/6/7 64 e 32 bit;
- Debian 5 64bit;
- Red Hat Ent. 2/3/4/5/6/7 32 e 64 bit;
- Ubuntu server Linux 64bit;
- SUN container Solaris 9 e 10.

Perimetro di attività (includere/non includere)

Il servizio di gestione sistemistica server Cloud comprende le seguenti attività:

- Installazione e configurazione delle componenti aggiuntive del sistema operativo, concordate preventivamente con i fornitori terzi, quali: DNS, IIS, DHCP, Antivirus, .NET, Ruolo AD, File Server, Printer Server;
- Aggiornamento del sistema operativo e dei software di base locale installati sui server, avendo cura di installare le patch e gli aggiornamenti di sicurezza proposti dal DPO (non sono incluse installazioni di nuove versioni di sistema operativo);
- Identificazione del malfunzionamento dei sistemi operativi e ricerca della sua causa attraverso un processo correttivo di eliminazione (troubleshooting);
- Gestione e aggiornamento del sistema locale antivirus dei server;
- Mantenimento del controllo degli accessi per proteggere e limitare gli interventi sui server solo agli end-user abilitati secondo le indicazioni fornite dall'Ente;
- Gestione delle utenze e dei relativi livelli di autorizzazione;
- Creazione e gestione delle policy di dominio;
- Gestione dei servizi di rete Microsoft connessi alle funzionalità del dominio (DNS, WINS);
- Predisposizione della struttura dello spazio disco utente (home directory escluse altre profilazioni legate a servizi di File server);
- Verifica della corretta esecuzione delle procedure di backup/restore;
- Hardening dei sistemi, ovvero messa in sicurezza del sistema attraverso la riduzione della sua superficie di attacco, con eventuale rimozione o disabilitazione di software o di username o di servizi non necessari.

Non rientrano nel servizio le seguenti attività:

- Installazione di nuove versioni di sistema operativo;
- Installazione di software non di base;
- Coordinamento interventi di manutenzione hw di competenza di terze parti;
- Distribuzione centralizzata dei sistemi operativi client e dei pacchetti applicativi;
- Supporto alle attività di inventory;
- Attività di Assessment del Sistema Informatico;
- Attività di progettazione e consolidamento infrastrutturale;
- Attività di consulenza sistemistica;
- Disaster Recovery delle basi dati, e dei sistemi;
- Estensioni temporanee degli orari standard di servizio o servizio di reperibilità;
- Stipula e gestione di contratti di fornitura e manutenzione hardware, software di base e applicativo e fornitura, sostituzione e conservazione dei supporti fisici utilizzati nell'attività di backup/restore sui server di proprietà del cliente;
- Servizi di reperibilità definibili secondo progetto ad hoc rispetto alle necessità del cliente.

Orari e livelli di servizio

| Servizio | Lunedì - Venerdì | Sabato - Domenica |
|--|------------------|-------------------|
| Servizio di gestione sistemistica server Cloud | 09.00 – 17.00 | - |

Non sono previsti livelli di servizio nell'erogazione del servizio di gestione sistemistica server Cloud.

Prerequisiti

Gestione Sicurezza VPC;

Assessment dei servizi che saranno ospitati sul VDC.

9.4.1.2 Servizi PaaS e DBaaS Gestiti**9.4.1.2.1 Oracle DBMS – High performance as a service****Descrizione del contesto tecnologico di riferimento**

Il servizio prevede la messa a disposizione di database su tecnologia Oracle. Il servizio può essere fornito in due varianti:

- database dedicato;
- database container con schemi dedicati in esecuzione su database Oracle condivisi.

Il Servizio Database viene erogato a bordo delle virtual farm del CSI Piemonte, istanziato su server virtuali con sistema operativo Linux in edizioni eterogenee, versioni supportate dal vendor o dalla community e aggiornate sia dal punto di vista funzionale che di sicurezza.

Oracle DBMS è disponibile nella versione 11g e superiori, in edizione ENTERPRISE. Sono escluse dalla configurazione standard le opzioni aggiuntive a pagamento.

Organizzazione per l'erogazione del servizio

Il Servizio RDBMS Oracle viene erogato con responsabilità e supervisione, sulla relativa infrastruttura, da parte dai sistemisti dell'Area Middleware e piattaforme infrastrutturali della Direzione Datacenter del CSI Piemonte.

Modalità di erogazione del servizio

Viene messo a disposizione uno schema di Oracle Database, su database server e istanze dedicate o condivise, con le caratteristiche richieste in termini di dimensioni e configurazione di storage per il database.

Di seguito le principali caratteristiche relative alla modalità di erogazione del servizio:

- è possibile la definizione di ulteriori utenze Oracle supplementari per eventuali esigenze di accesso ai dati;
- è garantita la possibilità di accesso da applicazioni web o da postazioni client/server in modo controllato e filtrato da apposite policy;
- Accesso amministrativo allo schema con privilegi completi sugli oggetti propri dello schema con possibilità di concessione privilegi agli eventuali utenti Oracle fruitori.
- Database server e istanza Oracle completamente gestiti e amministrati dai sistemisti della Direzione Datacenter del CSI Piemonte. Rientrano in queste competenze:
 - il backup dei dati e il mantenimento delle versioni storiche;
 - il monitoraggio della disponibilità infrastrutturale;
 - l'aggiornamento tecnologico e di sicurezza della piattaforma.

Eventuali richieste di supporto tecnico e di modifica della configurazione infrastrutturale del Servizio Database devono essere richiesti dal cliente tramite la funzione DEMAND della Direzione Datacenter.

Perimetro di attività (includere/non includere)

Attività incluse nel servizio:

- Gestione da parte dei sistemisti della Direzione Datacenter dell'istanza e del database Oracle;
- Gestione da parte dei sistemisti della Direzione Datacenter dei backup/restore dei dati e dell'archiviazione della serie storica dei backup;
- Gestione da parte dei sistemisti della Direzione Datacenter del sistema di monitoraggio del funzionamento del servizio database e della disponibilità di risorse computazionali e storage.

Attività escluse dal servizio:

- Accesso amministrativo allo schema dati tramite Sql*plus, SQL Developer e altri tool simili, in carico al cliente;
- Accesso ai dati, utilizzando qualsiasi libreria dei linguaggi client Oracle disponibili incluse le seguenti: Oracle Net (SQL*Net), JDBC, JSON e altri driver per accedere alle istanze messe a disposizione, effettuato da applicazioni completamente gestite dal cliente.

Orari e livelli di servizio

Il Servizio Oracle DBMS è disponibile 7 giorni su 7, H24, in modalità "best effort".

| Servizio | Lunedì - Venerdì | Sabato - Domenica |
|--|------------------|-------------------|
| Presidio sistemistico per il servizio RDBMS Oracle | 09.00 – 17.00 | - |

Informazioni minime per l'attivazione

- Documento di architettura applicativa e del servizio;

- Documento con specifiche tecniche e requisiti di configurazione;
- Moduli di richiesta RUTDB opportunamente compilati;
- Quantità di spazio disco ed eventuali specifiche di organizzazione logico-fisica, per il database schema;
- Previsioni di crescita nel tempo dello spazio disco occupato dal database schema;
- Quantità di spazio disco per aree di storage esterne al database schema;
- Previsioni di crescita nel tempo dello spazio disco occupato dalle aree di storage esterne al database schema;
- Eventuali policy di backup aggiuntive o difformi da quelle standard;
- Necessità di disporre di specifiche extended option Oracle;
- Necessità di integrare il sistema di alta affidabilità con funzioni di BC e DR;
- Numero di connessioni utente contemporanee previste.

Up-time garantito

99.8%

Tempi di consegna

5gg lavorativi

Metrica

- vCPU;
- vRAM;
- GB Storage DBMS Oracle.

9.4.1.2.2 Jboss as a service***Descrizione del contesto tecnologico di riferimento***

Il servizio prevede la messa a disposizione di istanze o partizioni dell'application server nelle versioni previste dalle pile tecnologiche del Consorzio. Nel servizio è compresa la gestione sistemistica e la possibilità di avvalersi di un supporto specialistico in caso di problematiche applicative di difficile individuazione.

Gli application server vengono istanziati su macchine virtuali, che a seconda delle esigenze di servizio possono essere dedicati oppure condivise.

Alla data attuale le versioni disponibili sono la 4.3 e la 6.4 EAP

Organizzazione per l'erogazione del servizio

Il servizio viene erogato con responsabilità e supervisione, sulla relativa infrastruttura, da parte dai sistemisti dell'Area Middleware e piattaforme infrastrutturali della Direzione Datacenter del CSI Piemonte

Le operazioni di rilascio in esercizio vengono effettuate seguendo il relativo processo aziendale dal gruppo Messa in Esercizio.

Il monitoraggio effettuato da Assistenza Operativa

I sistemisti Unix garantiscono la disponibilità della piattaforma tecnologica Vmware su cui si appoggiano le virtual machine.

Modalità di erogazione del servizio

Creazione nuovo ambiente

Le richieste di nuovi ambienti debbono essere sempre preventivamente concordate tramite apposita funzione aziendale (VARCH + Demand) in modo da effettuare la miglior scelta possibile in termini di risorse e sicurezza.

Una volta definito lo scenario:

- In caso di macchina dedicata richieste per allocazione indirizzi IP, registrazione dns e creazione VM;
- Creazione ambiente secondo lo standard definito per la versione scelta;
- Comunicazione a MIE dei parametri di riferimento per predisposizione monitoraggio.

Aumento risorse a disposizione

- Richiesta tramite remedy con indicazione delle necessità (cpu, memoria, disco, etc.);
- Valutazione richiesta in base alle risorse disponibili ed eventuale coinvolgimento della funzione di Demand Management.

Richieste supporto a troubleshooting

- Apertura Remedy con allegata descrizione della problematica;
- Se non allegabile alla remedy inviare email alla casella sistemisti-mdweb@csi.it con sintesi delle verifiche effettuate, descrizione dettagliata del problema e degli errori rintracciabili nei log che ne confermano la presenza. Se possibile allegare anche procedura per riprodurre il problema;
- Fornire indicazione dello sviluppatore che segue la problematica.

Perimetro di attività (include/non include)

Attività Incluse:

- Allestimento ambienti;
- Gestione sistemistica;
- Capacity planning;
- Performance Tuning (a richiesta);
- Supporto al troubleshooting;
- Patching (a richiesta).

Attività escluse:

- Gestione del servizio applicativo;
- Troubleshooting applicativo;
- Messa in esercizio applicazioni;
- Reperibilità.

Orari e livelli di servizio

Il servizio è erogato 7 giorni su 7, H24.

| Servizio | Lunedì - Venerdì | Sabato - Domenica |
|--|------------------|-------------------|
| Presidio sistemistico per il servizio JBoss as service | 09.00 – 17.00 | - |

Informazioni minime per l'attivazione

- Server name;
- Heap Max;
- Permanent memory;
- Spazio disco.
-

Up-time garantito

99,8% su base annuale

Tempi di consegna

3gg

Metrica

Memoria

9.4.2 SERVIZI DI END-POINT MANAGEMENT

Preventivo economico:

| Servizi di piattaforma infrastrutturali | Totale |
|---|-----------|
| Servizi di End-Point Management | 51.438,43 |

DESCRIZIONE

Il servizio viene proposto e può essere richiesto da tutti gli enti che necessitano un servizio di assistenza software alle postazioni di lavoro che comprenda anche l'intervento on-site presso l'utente. In particolare, si specifica che comprende i seguenti servizi: il servizio di customer service desk delle richieste di intervento, il servizio gestione asset, il servizio di coordinamento, il servizio di assistenza software remota, il servizio di assistenza software (on site o di presidio), sulle postazioni di lavoro, la gestione delle stampanti multifunzione, il servizio IMAC. Il costo del Servizio "Gestione PDL - Servizio On Site Standard" viene calcolato in funzione dei seguenti parametri (ne devono essere valorizzati almeno due su tre):

- Numero di pdl dell'ente: non viene richiesto un quantitativo minimo di postazioni per l'attivazione del servizio. Non sono previsti limiti di intervento sulle postazioni di lavoro per le richieste di malfunzionamento, mentre è previsto un limite/vincolo sulle richieste IMAC.
- Numero delle stampanti dipartimentali di rete e sulle apparecchiature in rete utilizzate dagli utenti (come scanner, plotter, ecc.): deve essere pari ad un minimo del 10% delle postazioni di lavoro gestite e ad un massimo del 15%, eventuali scostamenti verranno valutati in fase di offertazione.
- Presidio: viene erogato esclusivamente in quelle sedi in cui il numero delle postazioni di lavoro sia uguale o superiore alle 150 unità (a titolo di esempio: viene considerato 1 presidio fino ad un massimo di 450 postazioni di lavoro presenti), per quantitativi inferiori è possibile usufruire del servizio ad hoc di supporto specialistico (giornate a figure professionali) per il servizio di assistenza on site. La valutazione del numero delle sedi avviene in base alle postazioni di lavoro ivi presenti. I presidi, possono essere di due tipologie, fissi o mobili, per entrambe non è prevista la sostituzione delle risorse per i periodi di ferie o permessi spettanti. Nel primo caso le risorse impegnate e necessarie per garantire i livelli di servizi sono dislocate ed assegnate ad una sede specifica, nel secondo caso invece non sono dedicate ad una singola sede, ma garantiscono ed erogano il servizio sul perimetro richiesto.

TRATTAMENTO DEI DATI PERSONALI:

| | |
|---|--|
| Tipologia di dati che il servizio tratta | Dati personali |
| Tempo di conservazione dei dati | Log di accesso alla postazione (last user login, principal user) conservati per 6 mesi |
| Tempo di conservazione dei log di accesso o traffico | 6 mesi |
| Profilazione | utilizzo di sistemi di profilazione con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di profilazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |

| | |
|---|---|
| Autenticazione (ex autenticazione centralizzata) | utilizzo di sistemi di autenticazione (locali o nazionali) con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di autenticazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento (ex scansione vulnerabilità) | (es politiche di aggiornamento del software, test funzionale e di vulnerabilità del software utilizzato, limitazioni dell'accesso fisico al materiale che contiene dati personali,) |
| Backup e restore | Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup |

UTENTI ABILITATI AL SERVIZIO

I servizi di end-point management sono rivolti agli Enti della Pubblica Amministrazione e viene erogato agli utenti e ad eventuali collaboratori esterni autorizzati ad usufruire dei servizi sopra descritti.

Più precisamente possono accedere ai Servizi di End-Point Management:

- i dipendenti o gli utenti assegnatari o utilizzatori delle postazioni di lavoro inserite all'interno dell'asset comunicato al CSI-Piemonte;
- gli utenti (consulenti) esterni che sono autorizzati dall'ente a usufruire le postazioni di lavoro censite e comunicate al CSI-Piemonte come oggetto di assistenza.

Per permettere a ogni nuovo utente di accedere al servizio in oggetto sarà necessario che l'ente indichi e comunichi puntualmente al CSI-Piemonte ogni eventuale modifica sul personale autorizzato ad accedere al servizio.

MODALITÀ DI EROGAZIONE DEL SERVIZIO

Il servizio di assistenza software alle postazioni di lavoro viene erogato in due modalità: o da remoto, attraverso strumenti di controllo remoto della postazione, o on-site (se previsto) presso la postazione utente c/o l'ente.

MODALITÀ DI ACCESSO AL SERVIZIO

Per accedere ai servizi di assistenza software inerenti alle postazioni di lavoro gestite è possibile utilizzare i canali e le modalità indicate di seguito:

CANALI DI COMUNICAZIONE

| Servizio | Contatti | Orario di Servizio |
|---|--|---------------------------|
| Accoglienza delle chiamate (Contact Center) ed assistenza da remoto | Telefono: 011 316 8888 (salvo diversa comunicazione in fase di attivazione del servizio) E-mail: casella specifica dedicata al cliente (come comunicato all'ente in fase di attivazione del servizio) | Lun-Ven 8-18 |
| Assistenza on site | Viene attivata unicamente a seguito della chiamata al servizio di accoglienza | Lun-Giov 9-17 Ven 9-16 |

9.4.3 SERVIZI DI RETE E DI SICUREZZA ICT

Per la descrizione del servizio fare riferimento al documento "Catalogo e listino dei servizi del CSI",

Preventivo economico:

| Servizi di piattaforma infrastrutturali | Totale |
|---|--------------------|
| Servizi di Rete e di sicurezza ICT | € 11.938,39 |

Descrizione

Il CSI mette a disposizione soluzioni d'accesso a larga banda su tutto il territorio regionale tramite la Rete Unitaria per la Pubblica Amministrazione Regionale (RUPAR) e servizi di gestione completa in outsourcing delle infrastrutture di rete dati locali e geografiche e della telefonia, sia in forma tradizionale sia VoIP. I servizi di rete mettono a disposizione connettività di diverse tipologie, dalla navigazione Internet in modalità sicura ai collegamenti alla RUPAR per lo scambio dati con la PA Locale e con la PA Centrale attraverso il Sistema Pubblico di Connettività (SPC).

I Servizi di rete e sicurezza ICT comprendono:

| | | | |
|-------------------------------|--|--------------|------|
| Registrazione Domini Internet | Rinnovo dominio .it | Dominio | 1,00 |
| Registrazione Domini Internet | Attività di assistenza a dominio (gestione amministrativa + inserimento nel dsn) | Dominio | 1,00 |
| Certificati Web Server | Certificato standard SSL | Certificato | 1,00 |
| Certificati Web Server | Domini aggiuntivi (oltre il 1°) per certificato multidomain | Certificato | 1,00 |
| Gestione linee dati | Gestione_Linee_XDSL | Collegamento | 6,00 |
| Gestione linee dati | Gestione_Linee_FO | Collegamento | 1,00 |

| | | | |
|-----------------------------|---|-------------------|------|
| Sicurezza Perimetrale e VPN | Sicurezza perimetrale presso cliente – Advanced (fino a 200 utenti) | Q.tà apparati | 1,00 |
| Sicurezza Perimetrale e VPN | VPN IPSEC NON Gestita | Tunnel | 2,00 |
| Sicurezza Perimetrale e VPN | Rete 8 IP | Dimensione subnet | 2,00 |
| Sicurezza Perimetrale e VPN | Monitoraggio apparato di rete LAN Clienti | Q.tà apparati | 5,00 |
| Kit firma digitale | Fornitura nuovo kit di firma | Kit | 1,00 |
| Firma digitale remota | Dispositivo Otp: canone annuale per certificato associato | Certificato | 6,00 |

9.4.3.1 Gestione linee dati

Il servizio consiste nella gestione dei collegamenti dati di accesso alla RUPAR e ai suoi servizi di tipo xDSL e in fibra ottica, verifica e assegnazione del piano di indirizzamento IP RUPAR compatibile, monitoraggio e include il Customer Service Desk.

La componente di connessione e link dati è esclusa dal servizio e determinata da un apposito servizio ad hoc, a seconda della tipologia di acquisizione del servizio dati (tramite ad esempio convenzione SCR-SPC-CONSIP).

Trattamento dei dati personali:

N/A

Modalità di accesso al servizio

L'accesso al servizio per assistenza e supporto è il seguente:

| | |
|---|---|
| Telefono | 011 316 8888 |
| E-Mail | casella dedicata all'assistenza cliente |
| Disponibilità | Lun. – Ven. dalle 8.00 alle 18.00 |
| Presenza in carico richieste assistenza | Entro 2 ore lavorative |

La casella di assistenza è predisposta per le segnalazioni di malfunzionamenti ed attiva in modo automatico la procedura Remedy-HelpDesk.

Tempi di risoluzione Collegamenti convenzione SCR/Consip/CNIPA

Salvo casi di forza maggiore (intesi come eventi imprevedibili od eccezionali) entro 8 ore lavorative dall'apertura del guasto verso il fornitore o in funzione della convenzione al quale fa riferimento il collegamento dati in gestione.

In caso di finestra temporale del servizio di risoluzione guasti “Estesa” gli interventi di risoluzione saranno H24 (previa disponibilità di accesso ai locali e/o contatto con i referenti di sede utente).

9.4.3.2 Sicurezza perimetrale e VPN

Comprende:

9.4.3.2.1 Sicurezza perimetrale

Il servizio garantisce una separazione tra la rete locale dell’Ente e le reti esterne attraverso una soluzione di firewall a protezione del punto di interconnessione tra la LAN dell’Ente e la RUPAR; la soluzione è in grado di garantire un elevato grado di sicurezza, l’interoperabilità e l’interscambio applicativo; la soluzione offerta è graduale in funzione della complessità dei servizi da gestire e del throughput richiesto; può comprendere la messa a disposizione degli apparati necessari; il servizio include il Customer Service Desk.

Le motivazioni che portano alla necessità di disporre di un sistema di sicurezza perimetrale dedicato e personalizzato sono sintetizzabili nei seguenti punti:

- archivi presenti sulla rete dell’Ente contenenti dati privati/personali/sensibili;
- accesso in modo sicuro a servizi della RUPAR erogati dal CSI-Piemonte che coinvolgono la gestione/flussi di dati privati/personali/sensibili;
- protezione dei singoli posti di lavoro situati sulla rete interna dell’Azienda;
- possibilità di gestire sicurezza intra-LAN, con la creazione di VLAN, “separate” all’interno della stessa rete cliente;
- creazione di una porzione di rete protetta, DMZ, nella quale pubblicare eventuali servizi verso RUPAR/Internet.

Le caratteristiche tecniche del servizio di sicurezza offerto sono:

- servizio basato su piattaforma di firewall hardware, senza parti in movimento (hard disk o similari);
- elevati livelli di affidabilità (MTBF superiore ad analoghe soluzioni software);
- coprocessori dedicati al routing e alla crittografia (gestione del traffico cifrato IPSEC);
- gestione remotizzata presso il Centro Servizi per una maggiore velocità di intervento.

Livelli di servizio offerti CSI Piemonte:

- servizio attivo H24, 7 giorni su 7 con gestione operativa e sistemistica in orario lun.-ven. 8,30-17,30 (sabato, domenica e festivi esclusi);
- gestione (memorizzazione) dei logs generati dagli apparati;
- gestione di eventuali malfunzionamenti dell’apparato;
- costante e continuo aggiornamento delle funzionalità di protezione implementate dagli apparati.
- avvio comprensivo della fornitura dell’apparato hardware, delle attività di analisi e definizione delle policy, dell’installazione, della gestione ordinaria operativa erogata presso il Centro Servizi e delle manutenzioni hardware e software degli apparati.

TRATTAMENTO DEI DATI PERSONALI:

- Tipologia di dati che la piattaforma tratta: dati personali, si tratta dei log prodotti dalla piattaforma;
- Tempo di conservazione dei log di accesso o traffico: log di accesso e log del traffico conservati per 6 mesi;
- Tipologia di profilazione della piattaforma: amministratore e utente in sola lettura;
- Sicurezza del canale di comunicazione: https e ssh per l'amministrazione;
- Durata della conservazione dei dati: vedi sopra;
- Quali misure di sicurezza sono applicate ai dati personali e particolari (ovvero se la piattaforma applica la cifratura di dati oppure la pseudonimizzazione): conservazione dei dati cifrati.

| MISURA VERTICALE | DESCRIZIONE |
|--|---|
| Minimizzazione della quantità dei dati personali | rientrano misure di filtraggio e rimozione, riduzione della sensibilità attraverso la conversione, ridurre la natura identificativa del dato, ridurre l'accumulazione dei dati, limitare l'accesso ai dati |
| Profilazione | utilizzo di sistemi di profilazione con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di profilazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Autenticazione (ex autenticazione centralizzata) | utilizzo di sistemi di autenticazione (locali o nazionali) con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di autenticazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Utilizzo di sistemi di autenticazione multifattore | E previsto l'uso di certificati digitali, PIN, o autenticazione per l'autenticazione dell'utente e/o per i servizi di cooperazione applicativa |
| Gestione del ciclo di vita delle credenziali (ex scadenza credenziali) | gestione del ciclo del provisioning delle credenziali di autenticazione e della profilazione, in particolare della scadenza della credenziale (anche in termini di gestione delle segnalazioni da sistemi centralizzati) |
| Tracciabilità accessi risorse (ex tracciabilità accessi DB e audit log applicativi) | possibilità di tracciare accessi alle risorse critiche (es DB, front end e back end del servizio, share di rete critici) |
| Audit log applicativi | nel DB è prevista la tracciatura dell'identificativo utente che ha inserito/modificato i dati delle tabelle e si è in grado di risalire a chi e quando ha inserito/modificato/cancellato il record |
| Abilitazioni puntuali accessi DB (proxy SQL) | utilizzo di proxy SQL |

| | |
|---|--|
| Minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento (ex scansione vulnerabilità) | (es politiche di aggiornamento del software, test funzionale e di vulnerabilità del software utilizzato, limitazioni dell'accesso fisico al materiale che contiene dati personali,) |
| Cifratura del dato | mezzi implementati per assicurare la confidenzialità dei dati archiviati (in database, file, backup etc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di compromissione etc.) |
| Cifratura del canale | Applicazione di canale cifrato per le comunicazioni mediante utilizzo di protocolli HTTPS e SSH |
| Pseudonimizzazione | adozione di tecniche che garantiscono la non attribuzione a una persona identificata o identificabile di un dato ma consentono di identificare in un secondo momento i dati anche in maniera indiretta o da remoto (es conservando separatamente le informazioni che permettono di associare la persona al dato) |
| Backup e restore | Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup |
| Backup cifrati | utilizzo di sistemi per la cifratura dei backup |
| Business continuity/disaster recovery | esistenza di procedure per garantire la BC e/o il DR |

GESTIONE FILE DI LOG

Il servizio di sicurezza offerto dal CSI-Piemonte prevede la storicizzazione dei log in tempo reale presso il Centro Servizi di Gestione. I log vengono archiviati su sistema centralizzato, in conformità alle vigenti leggi, al fine di consentire all'autorità giudiziarie incaricate, di poter acquisire informazioni utili per eventuali indagini che dovessero coinvolgere i servizi erogati.

UTENTI ABILITATI AL SERVIZIO

Servizio rivolto agli Enti della Pubblica Amministrazione regionale piemontese.

Modalità di accesso al servizio

Il servizio è comprensivo della fornitura di un apparato hardware (Juniper SSG 140) con prestazioni e funzionalità conformi alle esigenze dell'Ente, delle attività di analisi e definizione delle policy, dell'installazione, della gestione ordinaria operativa erogata presso il Centro Servizi e delle manutenzioni hardware e software degli apparati.

Le comunicazioni inerenti la segnalazione di guasti o la richiesta di modifica policy devono essere effettuate verso il Contact Center del CSI secondo le modalità concordate con l'ente.

La storicizzazione dei log, in tempo reale presso il Centro Servizi del CSI, avviene mediante archiviazione su un sistema centralizzato, in conformità alle vigenti leggi, al fine di consentire all'autorità giudiziarie incaricate, di poter acquisire informazioni utili per eventuali indagini che dovessero coinvolgere i servizi erogati.

Il servizio di Sicurezza perimetrale comprende un corrispettivo per le attività di predisposizione che contempla un assessment ed un canone di servizio per le attività di gestione ordinaria.

Il cliente è tenuto a fornire le indicazioni puntuali delle policy con porte, IP e protocollo. Ogni ulteriore approfondimento è fornito da tecnici specializzati attraverso i servizi professionali di supporto specialistico.

MODALITÀ DI EROGAZIONE DEL SERVIZIO

Il servizio viene erogato agli Enti che hanno connettività RUPAR.

L'accesso al servizio per assistenza e supporto è il seguente:

| | |
|---|---|
| Telefono | 011 316 8888 |
| E-Mail | casella dedicata all'assistenza cliente |
| Disponibilità | Lun. – Ven. dalle 8.00 alle 17.00 |
| Presenza in carico richieste assistenza | Entro 2 ore lavorative |

GESTIONE ORDINARIA DEL SERVIZIO

- **tempo di intervento su richiesta di modifica di policy e/o configurazioni dell'apparato di sicurezza:** entro 3 gg lavorativi inteso come tempo intercorrente tra la richiesta al centro di Help-Desk del CSI-Piemonte secondo le modalità previste e la verifica e realizzazione della richiesta, effettuata da remoto. Le richieste dovranno essere inviate alla casella dedicata all'assistenza cliente o al numero telefonico 011-316.88.88;
- **sostituzione dell'apparato in caso di guasto:** entro 3 gg lavorativi, intesi come il tempo intercorrente tra la segnalazione del disservizio e la presenza presso la sede del cliente dei tecnici preposti al ripristino del disservizio;
- **aggiornamenti release software:** il servizio prevede il costante aggiornamento del software a protezione della rete del Cliente; l'applicazione delle nuove release sarà comunicata preventivamente (almeno una settimana prima dell'intervento) alla casella di posta elettronica del referente del Cliente, oppure su specifica richiesta del cliente concordate con lo stesso, fermo restando che il disservizio non sarà indicativamente superiore ai 10 minuti.

9.4.3.2.2 VPN IPSec e VPN SSL

Il servizio **VPN IPSec** fornisce un tunnel sicuro per lo scambio dati ai committenti che abbiano necessità di collegarsi alla RUPAR per l'espletamento di procedure di scambio con altre Pubbliche Amministrazioni; la soluzione è disponibile in modalità "Gestita" con messa a disposizione e configurazione delle due terminazioni a carico di CSI oppure "Non gestita" dove la gestione della terminazione lato cliente è a carico dell'Ente. Il servizio include il Customer Service Desk.

Il servizio **VPN SSL** consiste nella configurazione e gestione di un accesso ai Data Center del Consorzio in modalità sicura mediante web browser per i committenti che necessitano di svolgere

attività di assistenza sistemistica o applicativa. Il servizio include il Customer Service Desk. Si tratta di un Servizio di tunnel su Internet sicuro (cifrato) per lo scambio dati.

MODALITÀ DI EROGAZIONE

La seguente tabella illustra in maniera schematica la proposta delle differenti tipologie di VPN:

| | | |
|------|-----------------------|--|
| VP01 | VPN IPSEC Gestita | VPN IPSEC per l'accesso alla SF in modalità sicura mediante terminatore CSI concesso come servizio |
| VP02 | VPN IPSEC NON Gestita | VPN IPSEC per l'accesso alla SF in modalità sicura mediante terminatore del cliente |
| VP03 | VPN SSL | VPN SSL per l'accesso alla SF in modalità sicura attraverso Web Browser |

UTENTI ABILITATI AL SERVIZIO

Servizio rivolto agli Enti della Pubblica Amministrazione regionale piemontese.

MODALITÀ DI EROGAZIONE DEL SERVIZIO

Il servizio viene erogato agli Enti che hanno connettività INTERNET.

L'accesso al servizio per assistenza e supporto è il seguente:

| | |
|---|---|
| Telefono | 011 316 8888 |
| E-Mail | casella dedicata all'assistenza cliente |
| Disponibilità | Lun. – Ven. dalle 8.00 alle 17.00 |
| Presenza in carico richieste assistenza | Entro 2 ore lavorative |

Di seguito sono indicati le diverse proposte di virtual private network.

VPN IPSEC NON GESTITA

Questo servizio fornisce un tunnel sicuro sempre disponibile per lo scambio dati, pertanto è adatto agli Enti che abbiano necessità di trasmettere o ricevere dati in maniera continuativa.

Può essere offerto a tutti gli Enti che, disponendo di una loro rete gestita ma non collegata alla RUPAR, hanno necessità di collegarsi alla RUPAR per l'espletamento di procedure di scambio dati con la Pubblica Amministrazione.

La soluzione si applica per gli Enti che hanno competenza nella configurazione dell'IPSEC in quanto è a loro carico la configurazione del loro terminatore.

L'Ente deve disporre di una propria rete locale, di un accesso Internet e di un proprio terminatore IPSEC.

Il servizio prevede la configurazione del terminatore CSI e della comunicazione via mail dei parametri all'Ente, ed è a suo carico la configurazione del proprio terminatore.

Non è previsto il supporto al cliente per la configurazione in loco del proprio terminatore, ma è previsto un supporto telefonico.

È responsabilità dell'Ente comunicare e/o rinnovare eventuali variazioni di accesso e/o utilizzo del canale IPSEC attivato.

L'attivazione del servizio è preceduta da una attività di verifica e assessment a progetto sulle necessità della tipologia di connessione e accesso della VPN.

Per ARPEA, il CSI Piemonte mantiene i seguenti tunnel IPsec:

- **vpn.arpea-agea.**
- **arpea.tim.it** a supporto dell'APN che raccoglie il traffico dei cellulari, realizzato a fine 2018, e per il quale è previsto un costo di start-up all'interno della presente CTE

Indirizzi IP pubblici: servizio di messa a disposizione di indirizzi IP pubblici degli Autonomous System del CSI per l'esposizione di servizi direttamente sulla rete Internet.

Gli indirizzi IP pubblici sono messi a disposizione del Cliente per il periodo concordato nella specifica offerta di servizio e subordinati alla sottoscrizione del modulo di assunzione di responsabilità da allegare all'offerta

La proprietà degli indirizzi IP pubblici assegnati, rimarrà comunque del CSI Piemonte e al termine del servizio torneranno in uso al Consorzio.

Le subnet assegnate ad ARPEA sono le seguenti:

- 158.102.57.224/29
- 158.102.224.24/29

9.4.3.3 Certificati WEB Server

Servizio di fornitura di certificati SSL firmati da un soggetto terzo di fiducia (trusted third part), abilitato ad emettere un certificato digitale tramite una procedura di certificazione che segue standard internazionali e in conformità alla normativa europea e nazionale in materia.

SSL o "Secure Sockets Layer" è un protocollo progettato per consentire alle applicazioni di trasmettere informazioni in modo sicuro e protetto grazie all'invio e la ricezione di chiavi di protezione e della criptatura/decriptatura delle informazioni trasmesse utilizzando le stesse chiavi.

Il servizio è disponibile in versioni con ampiezza di utilizzo diversificate e include il Customer Service Desk.

TRATTAMENTO DEI DATI PERSONALI:

- Tipologia di dati che la piattaforma tratta: la piattaforma tratta dati anagrafici degli utenti che richiedono il rilascio di un certificato Web Server
- Tempo di conservazione dei log di accesso o traffico: n.a.
- Tipologia di profilazione della piattaforma: n.a.
- Sicurezza del canale di comunicazione: n.a.
- Durata della conservazione dei dati: n.a.

| Misura verticale | Descrizione |
|-----------------------------|--|
| Profilazione | utilizzo di sistemi di profilazione con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di profilazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). Viene registrato e comunicato al fornitore del servizio il nominativo e l'Ente di pertinenza di chi ha richiesto l'emissione del certificato. |
| Cifratura del canale | Applicazione di canale cifrato per le comunicazioni mediante utilizzo di protocolli HTTPS e SSH |

9.4.3.4 Registrazione domini internet

CSI offre ai committenti il servizio di registrazione dei domini internet con le possibili estensioni (.it, .com, .mobi, .eu, .biz, .net, .info, .org, .travet, .tv); i domini hanno scadenza annuale. È inoltre disponibile l'assistenza per la gestione amministrativa e per la registrazione dsn (Data Source Name).

Il dominio richiesto, se libero, viene registrato nei DNS del CSI-Piemonte e poi presso il fornitore.

I domini hanno scadenza annuale: quelli con primo livello .it vengono automaticamente rinnovati alla scadenza a meno che non venga comunicato altrimenti, mentre per gli altri è necessario richiedere specificatamente il rinnovo.

TRATTAMENTO DEI DATI PERSONALI:

- Tipologia di dati che la piattaforma tratta: la piattaforma tratta dati anagrafici degli utenti che richiedono la registrazione di un dominio internet
- Tempo di conservazione dei log di accesso o traffico: n.a.
- Tipologia di profilazione della piattaforma: n.a.
- Sicurezza del canale di comunicazione: n.a.
- Durata della conservazione dei dati: n.a.

TRATTAMENTO DEI DATI PERSONALI:

| | |
|---------------------|---|
| Profilazione | utilizzo di sistemi di profilazione con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di profilazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). Viene registrato e comunicato al fornitore del servizio il nominativo e l'Ente di pertinenza di chi ha richiesto la registrazione del dominio. |
|---------------------|---|

UTENTI ABILITATI AL SERVIZIO

Servizio rivolto agli Enti Locali Consorziati sia direttamente che attraverso Ente sovraordinato (Provincia o Unione) al CSI Piemonte.

MODALITÀ DI ACCESSO AL SERVIZIO

Il servizio viene erogato agli Enti che hanno connettività INTERNET.

CANALI DI COMUNICAZIONE

Per le richieste di assistenza riguardanti i servizi di certificati web server o domini internet, il Cliente dovrà utilizzare i canali mail o telefonici dell'hd generico di competenza per la propria tipologia di Ente (es. hd_comune@csi.it per il Comune di Torino, hd_agenzie@csi.it per AIPO, hd_entilocali@csi.it per i comuni, le province e le unioni di comuni...): il Contact Center di primo livello procederà ad aprire un ticket verso il gruppo di servizio corretto.

Assistenza telefonica:

| Servizio | Lunedì - Venerdì | Sabato - Domenica |
|-------------------------------------|------------------|-------------------|
| Servizio assistenza 011 316 8888 | 08.00 - 17.00 | - |

9.4.3.5 Kit firma digitale

Il servizio consiste nella messa a disposizione di un kit di firma digitale che consente di scambiare in rete documenti con piena validità legale. Possono dotarsi di firma digitale tutte le persone fisiche: cittadini, amministratori e dipendenti di società e pubbliche amministrazioni; il servizio include il Customer Service Desk.

TRATTAMENTO DEI DATI PERSONALI:

- tipologia di dati che la piattaforma tratta: dati personali, si tratta dei log prodotti dalla piattaforma
- tempo di conservazione dei log di accesso o traffico: log di accesso e log del traffico conservati per 6 mesi
- tipologia di profilazione della piattaforma: amministratore e utente in sola lettura
- sicurezza del canale di comunicazione: https e ssh per l'amministrazione
- Durata della conservazione dei dati: vedi sopra
- Quali misure di sicurezza sono applicate ai dati personali e particolari (ovvero se la piattaforma applica la cifratura di dati oppure la pseudonimizzazione): conservazione dei dati cifrati.

| Misura verticale | Descrizione |
|---------------------|--|
| Profilazione | utilizzo di sistemi di profilazione con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di profilazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |

| | |
|---|---|
| Autenticazione (ex autenticazione centralizzata) | utilizzo di sistemi di autenticazione (locali o nazionali) con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di autenticazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Utilizzo di sistemi di autenticazione multifattore | E previsto l'uso di certificati digitali, PIN, o autenticazione per l'autenticazione dell'utente e/o per i servizi di cooperazione applicativa |
| Gestione del ciclo di vita delle credenziali (ex scadenza credenziali) | gestione del ciclo del provisioning delle credenziali di autenticazione e della profilazione, in particolare della scadenza della credenziale (anche in termini di gestione delle segnalazioni da sistemi centralizzati) |
| Tracciabilità accessi risorse (ex tracciabilità accessi DB e audit log applicativi) | possibilità di tracciare accessi alle risorse critiche (es DB, front end e back end del servizio, share di rete critici) |
| Minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento (ex scansione vulnerabilità) | (es politiche di aggiornamento del software, test funzionale e di vulnerabilità del software utilizzato, limitazioni dell'accesso fisico al materiale che contiene dati personali,) |
| Cifratura del dato | mezzi implementati per assicurare la confidenzialità dei dati archiviati (in database, file, backup etc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di compromissione etc.) |
| Cifratura del canale | Applicazione di canale cifrato per le comunicazioni mediante utilizzo di protocolli HTTPS e SSH |
| Backup e restore | Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup |
| Backup cifrati | utilizzo di sistemi per la cifratura dei backup |
| Business continuity/disaster recovery | esistenza di procedure per garantire la BC e/o il DR |

9.4.3.6 Firma digitale remota

Il servizio di firma digitale remota si colloca nell'ambito dei servizi di rilascio di strumenti abilitanti alla formale dematerializzazione dei documenti. Il servizio ha lo scopo di rilasciare agli utenti della PA un certificato di firma digitale qualificata che risiede su un server remoto securizzato, presso il Certificatore (accreditato AgID).

Il servizio comprende la gestione di certificati di firma remota qualificati secondo quanto previsto nella deliberazione del Centro nazionale per l'informatica nella pubblica amministrazione n. 45 del 21 maggio 2009 e sue successive modificazioni con provisioning / deprovisioning dei certificati digitali e dei dispositivi di accesso durante il loro "ciclo" di vita ossia la attivazione, la sospensione ed eventuale revoca.

I dispositivi One Time Password, dotati di chip e schermo LCD, generano una password con valore momentaneo, valida per la sessione di firma e non riutilizzabile; il software del dispositivo One Time Password è resa disponibile per apparati mobili dotati di sistema operativo Android, iOS, WindowsMobile nelle versioni più recenti. Il codice di attivazione della firma, in alternativa, può essere inviato tramite messaggio SMS al numero telefonico indicato dall'utente titolare in fase di registrazione dello stesso.

Il servizio di rilascio dei certificati di firma digitale è reso disponibile agli enti tramite riconoscimento *de visu* dell'utente finale e consegna delle credenziali di accesso.

Il certificato di firma digitale remota potrà essere utilizzato tramite appositi strumenti software che prevedono la generazione di documenti muniti di firma digitale qualificata, erogati dal CSI o dal Certificatore che ha rilasciato il certificato stesso.

TRATTAMENTO DEI DATI PERSONALI:

Sulla piattaforma i dati oggetto di firma remota sono le "impronte" dei documenti, ovvero le stringhe di hash calcolate sui file originari, e non richiedono pertanto l'applicazione di pseudonimizzazione o una cifratura aggiuntiva.

| | |
|---|---|
| Tipologia di dati che il servizio tratta | Dati personali |
| Tempo di conservazione dei dati | <ul style="list-style-type: none"> • tempo di conservazione dei log di accesso o traffico: 24 mesi • Durata della conservazione dei dati: 20 anni |
| Tempo di conservazione dei log di accesso o traffico | 6 mesi |
| Profilazione | utilizzo di sistemi di profilazione con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di profilazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Autenticazione (ex autenticazione centralizzata) | utilizzo di sistemi di autenticazione (locali o nazionali) con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di autenticazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Utilizzo di sistemi di autenticazione multifattore | E previsto l'uso di certificati digitali, PIN, o autenticazione per l'autenticazione dell'utente e/o per i servizi di cooperazione applicativa |
| Gestione del ciclo di vita delle credenziali (ex scadenza credenziali) | gestione del ciclo del provisioning delle credenziali di autenticazione e della profilazione, in particolare della scadenza della credenziale (anche in termini di gestione delle segnalazioni da sistemi centralizzati) |

| | |
|---|--|
| Tracciabilità accessi risorse (ex tracciabilità accessi DB e audit log applicativi) | possibilità di tracciare accessi alle risorse critiche (es DB, front end e back end del servizio, share di rete critici) |
| Minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento (ex scansione vulnerabilità) | (es politiche di aggiornamento del software, test funzionale e di vulnerabilità del software utilizzato, limitazioni dell'accesso fisico al materiale che contiene dati personali,) |
| Cifratura del dato | mezzi implementati per assicurare la confidenzialità dei dati archiviati (in database, file, backup etc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di compromissione etc.) |
| Cifratura del canale | Applicazione di canale cifrato per le comunicazioni mediante utilizzo di protocolli HTTPS e SSH |
| Backup e restore | Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup |
| Backup cifrati | utilizzo di sistemi per la cifratura dei backup |
| Business continuity/disaster recovery | esistenza di procedure per garantire la BC e/o il DR |

UTENTI ABILITATI AL SERVIZIO

Funzionari e dirigenti della Pubblica Amministrazione.

MODALITÀ DI ACCESSO AL SERVIZIO

Gli strumenti per l'apposizione di una firma digitale remota sono: il software client (per s.o. Windows) messo a disposizione dal certificatore o il software DWD-Libro Firma erogato dal CSI-Piemonte via web e accessibile dall'intranet dell'ente utilizzatore. Per fruire del servizio di firma remota l'utente riceve una "one time password (OTP)" tramite SMS sul proprio telefono o generata su token fisico (chiavetta).

CANALI DI COMUNICAZIONE

La gestione operativa osserva il seguente orario:

| Servizio | Lunedì - Giovedì | Venerdì | Sabato - Domenica |
|--|--------------------------------|--------------------------------|-------------------|
| Gestione Operativa: hd_firmadigitale@csi.it | 09.00 - 12.30 14.30 - 17.00 | 09.00 - 12.30 14.30 - 16.00 | - |

9.5 SERVIZI DI PIATTAFORMA SUPPORTO E COOPERAZIONE

9.5.1 AUTOMAZIONE PROCESSI DI INPUT/OUTPUT

Per la descrizione del servizio fare riferimento al documento "Catalogo e listino dei servizi del CSI".

Preventivo economico:

| Servizi di piattaforma supporto e cooperazione | Totale |
|--|-----------------|
| Automazione processi di input/output | € 120,00 |
| TOTALE | € 120,00 |

Il servizio è stato dimensionato in riferimento alle seguenti voci:

- Pagine stampate (stimate in 8.000);
- Modulo/template utilizzato: 1 modulo.

TRATTAMENTO DEI DATI PERSONALI:

| | |
|--|---|
| Tipologia di dati che il servizio tratta | La piattaforma non ha persistenza di dati, ma i vari applicativi fruitori inviano ai loro destinatari i loro dati attraverso la piattaforma |
| Tempo di conservazione dei dati | la piattaforma non ha dati persistenti ovvero non storicizza i dati al suo interno: i dati transitano in piattaforma e poi vengono cancellati con processi automatizzati secondo le politiche di svecchiamento degli applicativi fruitori |
| Tempo di conservazione dei log di accesso o traffico | I log della piattaforma vengono conservati per 12 mesi |
| Ulteriori misure tecniche di sicurezza applicate | la piattaforma non applica alcuna cifratura sui dati che “transitano” attraverso la piattaforma stessa, la cifratura è onere degli applicativi fruitori |
| Minimizzazione della quantità dei dati personali | rientrano misure di filtraggio e rimozione, riduzione della sensibilità attraverso la conversione, ridurre la natura identificativa del dato, ridurre l'accumulazione dei dati, limitare l'accesso ai dati |
| Profilazione | utilizzo di sistemi di profilazione con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di profilazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Autenticazione (ex autenticazione centralizzata) | utilizzo di sistemi di autenticazione (locali o nazionali) con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di autenticazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Gestione del ciclo di vita delle credenziali (ex scadenza credenziali) | gestione del ciclo del provisioning delle credenziali di autenticazione e della profilazione, in particolare della scadenza della credenziale (anche in termini di gestione delle segnalazioni da sistemi centralizzati) |
| Tracciabilità accessi risorse (ex tracciabilità accessi DB e audit log applicativi) | possibilità di tracciare accessi alle risorse critiche (es DB, front end e back end del servizio, share di rete critici) |

| | |
|---|--|
| Minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento (ex scansione vulnerabilità) | (es politiche di aggiornamento del software, test funzionale e di vulnerabilità del software utilizzato, limitazioni dell'accesso fisico al materiale che contiene dati personali,) |
| Cifratura del dato | mezzi implementati per assicurare la confidenzialità dei dati archiviati (in database, file, backup etc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di compromissione etc.) |
| Cifratura del canale | Applicazione di canale cifrato per le comunicazioni mediante utilizzo di protocolli HTTPS e SSH |
| Pseudonimizzazione | adozione di tecniche che garantiscono la non attribuzione a una persona identificata o identificabile di un dato ma consentono di identificare in un secondo momento i dati anche in maniera indiretta o da remoto (es conservando separatamente le informazioni che permettono di associare la persona al dato) |
| Backup e restore | Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup |
| Backup cifrati | utilizzo di sistemi per la cifratura dei backup |
| Business continuity/disaster recovery | esistenza di procedure per garantire la BC e/o il DR |

9.5.2 IDENTITY & ACCESS

Per la descrizione del servizio fare riferimento al documento “Catalogo e listino dei servizi del CSI”.

Preventivo economico:

| Servizi di piattaforma supporto e cooperazione | Totale |
|--|-------------------|
| Identity & Access | € 1.895,52 |
| TOTALE | € 1.895,52 |

Il servizio è stato dimensionato in riferimento a 2 unità di installazione.

DESCRIZIONE:

Nella piattaforma di Identity & Access sono contemplate tutte le attività di gestione del processo di autenticazione e autorizzazione degli utenti per l'utilizzo di servizi telematici, siano essi dipendenti o collaboratori dei committenti oppure cittadini e/o imprese. In particolare la piattaforma si occupa di:

- Gestire gli IdP (Identity Provider) locali, controllo delle misure di sicurezza e del rispetto dei criteri e delle regole previsti dalla normativa e dal Codice in materia di protezione dei dati personali;
- Gestione delle configurazioni e dell'integrazione verso gli IdP esterni;
- Gestione dell'infrastruttura tecnologica che stabilisce le policy e le abilitazioni (ruoli e attributi) dei dipendenti della pubblica amministrazione locale.

- Gestione dell'infrastruttura tecnologica che stabilisce le policy e le abilitazioni di cittadini e imprese che utilizzano i servizi telematici erogati dalle amministrazioni.

TRATTAMENTO DEI DATI PERSONALI:

- tipologia di dati che la piattaforma tratta: Dati anagrafici dei soggetti a cui vengono rilasciate le credenziali
- tempo di conservazione dei log di accesso o traffico: 36 mesi
- tipologia di profilazione della piattaforma: Amministratore, Operatore di Back Office, Utente
- sicurezza del canale di comunicazione: HTTPS
- Durata della conservazione dei dati: i dati utente non vengono mai cancellati a meno di specifica richiesta dell'utente medesimo
- Quali misure di sicurezza sono applicate ai dati personali e particolari (ovvero se la piattaforma applica la cifratura di dati oppure la pseudonimizzazione): la piattaforma prevede la criptazione dei dati

| Misura verticale | Descrizione |
|---|--|
| Profilazione | utilizzo di sistemi di profilazione con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di profilazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento). |
| Utilizzo di sistemi di autenticazione multifattore | E' previsto l'uso di certificati digitali, PIN, o autenticazione per l'autenticazione dell'utente e/o per i servizi di cooperazione applicativa |
| Audit log applicativi | nel DB è prevista la tracciatura dell'identificativo utente che ha inserito/modificato i dati delle tabelle e si è in grado di risalire a chi e quando ha inserito/modificato/cancellato il record |
| Cifratura del dato | mezzi implementati per assicurare la confidenzialità dei dati archiviati (in database, file, backup etc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di compromissione etc.) |
| Cifratura del canale | Applicazione di canale cifrato per le comunicazioni mediante utilizzo di protocolli HTTPS e SSH |
| Backup cifrati | utilizzo di sistemi per la cifratura dei backup |

| Servizio IT | ALO | TOTALE Figure Professionali | TOTALE IMPORTO Figure Professionali | ACCOUNT | BUSINESS ANALYST | BUSINESS INFORMATION MANAGER | DATA ADMINISTRATOR | DATA SPECIALIST | DEVELOPER | DIGITAL EDUCATOR | DIGITAL MEDIA SPECIALIST | GIS SPECIALIST | GOVERNANCE SPECIALIST | INFORMAT SECURITY SPECIALIST | IT GOVERNANCE PARTNER | LAND/GEOMATIC S SURVEYOR | PROJECT MANAGER | SERVICE SPECIALIST | SERVICE SUPPORT | SOLUTION DESIGNER | SYSTEM ADMINISTRATOR | SYSTEM ANALYST | SYSTEM ARCHITECT | TECHNICAL SPECIALIST | UX DESIGNER | |
|--|--|-----------------------------|-------------------------------------|---------|------------------|------------------------------|--------------------|-----------------|-----------|------------------|--------------------------|----------------|-----------------------|------------------------------|-----------------------|--------------------------|-----------------|--------------------|-----------------|-------------------|----------------------|----------------|------------------|----------------------|-------------|------|
| Supporto specialistico direzionale | Flussi Documentali e dematerializzazione | 5 | 2.020,00 € | 0,00 | 5,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 |
| Altri servizi ad hoc | Flussi Documentali e dematerializzazione | 35 | 12.264,00 € | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 7,00 | 14,00 | 14,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 |
| Gestione operativa applicazioni: Assistenza funzionale | 2018 - ALO - Comunicazione e Accesso MUI | 2 | 728,50 € | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,50 | 1,00 | 0,50 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 |
| Asset, Compliance e Security Management | | 2 | 971,00 € | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 1,00 | 0,00 | 1,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 |
| Elaborazione, integrazione e gestione dati e contenuti | Web | 6 | 1.794,00 € | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 |
| Altri servizi ad hoc | Gestione rete fonia | 31 | 11.005,00 € | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 31,00 | 0,00 | 0,00 | 0,00 | 0,00 |
| Supporto specialistico operativo | Servizi contabili | 5 | 2.020,00 € | 0,00 | 5,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 |
| Governo | | 119 | 55.472,00 € | 15,00 | 2,00 | 27,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 24,00 | 0,00 | 29,00 | 0,00 | 12,00 | 0,00 | 0,00 | 0,00 | 0,00 | 10,00 | 0,00 | 0,00 | 0,00 | 0,00 |
| Supporto specialistico operativo | Servizio di Disaster Recovery e test) | 34 | 12.378,00 € | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 4,00 | 0,00 | 0,00 | 0,00 | 30,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 |
| Altri servizi ad hoc | DPS V Ass Supp ISO27000 | 40 | 17.280,00 € | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 40,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 |
| Elaborazione, integrazione e gestione dati e contenuti | Territorio | 3,5 | 1.297,50 € | 0,00 | 0,00 | 0,50 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,50 | 0,00 | 0,00 | 0,00 | 0,00 | 2,50 | 0,00 | 0,00 | 0,00 | 0,00 |

TABELLA CON IL DETTAGLIO DEI SERVIZI A MISURA PREVISTI IN CTE

| Servizi di piattaforma applicativi | | | | | |
|--|-----------------|---|---------------------|-----------------------------|----------------------|
| Servizio | Voce di Listino | Unità di Misura | Volumi preventivati | Importo per unità di misura | Importo preventivato |
| Contabilità | | Fascia 1 Mandati | 1300 | 2,5 | 3250 |
| Contabilità | | Fascia 1 Capitoli/Articolo | 100 | 2,5 | 250 |
| Contabilità | | Fascia 1 Accertamenti/impegni | 600 | 2,5 | 1500 |
| Contabilità | | Fascia 1 Utenti | 5 | 100,0 | 500 |
| Posta Elettronica e Servizi di Comunicazione Unificata | | Profilo Standard Servizi base di posta elettronica + serv non opzic | 88 | 11,6 | 1023,6 |
| Posta Elettronica e Servizi di Comunicazione Unificata | | Assistenza Avanzata | 113 | 9,2 | 1036,74 |
| Posta Elettronica e Servizi di Comunicazione Unificata | | Profilo Premium Servizi base di posta elettronica + serv non opzic | 25 | 24,9 | 623,16 |
| Posta Elettronica e Servizi di Comunicazione Unificata | | Servizi opzionali Drive | 10 | 0,8 | 7,56 |
| Posta Elettronica e Servizi di Comunicazione Unificata | | Servizi opzionali Storage Aggiuntivo | 140 | 0,8 | 105,3 |
| Posta Elettronica e Servizi di Comunicazione Unificata | | Servizi opzionali Archivio posta on-line | 300 | 0,8 | 225,61 |
| Posta Elettronica e Servizi di Comunicazione Unificata | | Servizi opzionali Backup online | 290 | 3,5 | 1003,2 |
| Posta Elettronica e Servizi di Comunicazione Unificata | | Servizi opzionali Archivio replica+NAS | 300 | 2,0 | 607,68 |
| Posta Elettronica e Servizi di Comunicazione Unificata | | Gestione utenze e profili di accesso | 1 | 1,5 | 1,55 |
| PEC - Posta Elettronica Certificata | | Casella: Assistenza Standard | 2 | 4,6 | 9,14 |
| PEC - Posta Elettronica Certificata | | Casella PEC Articolata - Massiva | 1 | 450,6 | 450,6 |
| PEC - Posta Elettronica Certificata | | Casella: Assistenza Evoluta | 2 | 17,1 | 34,18 |
| PEC - Posta Elettronica Certificata | | Caselle PEC Articolata - Standard (1 GB + 1 GB) | 1 | 10,5 | 10,51 |
| Dematerializzazione | | Utenti registrati sul sistema DoQui Acta | 70 | 40,6 | 2842 |
| Dematerializzazione | | Numero di invii e ricezioni dalle caselle PEC | 11003 | 0,7 | 8142,22 |
| Dematerializzazione | | Gigabyte di spazio disco - ADVANCED | 149 | 238,6 | 35551,4 |
| Telemaco | | Quota fissa fino a 250 consultazioni | 1 | 175,0 | 175 |
| Telemaco | | Singola consultazione aggiuntiva oltre le 250 | 1755 | 0,7 | 1228,5 |
| Fatturazione Elettronica | | Quota fissa Servizio Base | 0 | 900,0 | 0 |
| Fatturazione Elettronica | | Numero fatture passive ed active-Servizio Base | 310 | 2,2 | 669,6 |
| Servizi al Personale | | Cedolini/Mese - 0-100 | 740 | 2,6 | 1924 |
| Servizi al Personale | | DWH - Cedolini Unica | 740 | 0,2 | 155,4 |
| Servizi al Personale | | Credenziali | 2 | 5,4 | 10,72 |
| Sito Web | | Numero siti | 1 | 2.940,0 | 2940 |
| Servizi al Personale | | Cedolini/Mese - unica fascia | 740 | 0,5 | 370 |
| Servizi al Personale | | Cedolini/Mese - 0-100 | 740 | 1,8 | 1332 |

| Servizi di piattaforma Supporto e Cooperazione | | | | | |
|--|-----------------|---------------------------|---------------------|-----------------------------|----------------------|
| Servizio | Voce di Listino | Unità di Misura | Volumi preventivati | Importo per unità di misura | Importo preventivato |
| Identity & Access | | Unità d'Installazione | 2 | 947,8 | 1895,52 |
| Automazione processi di input/output | | Numero di pagine stampate | 8000 | 0,0 | 120 |

| Servizi di piattaforma infrastrutturale | | | | | |
|---|--|---|---------------------|-----------------------------|----------------------|
| Servizio | Voce di Listino | Unità di Misura | Volumi preventivati | Importo per unità di misura | Importo preventivato |
| Servizi di Rete e di Sicurezza ICT | | dominio .it | 1 | 4,96 | 4,96 |
| Servizi di Rete e di Sicurezza ICT | | Gestione amministrativa + inserimento nel dsn a dom | 1 | 30,00 | 30 |
| Servizi di Rete e di Sicurezza ICT | | Gestione_Monitoraggio_FO | 1 | 768,00 | 770,11 |
| Servizi di Rete e di Sicurezza ICT | | Gestione_Monitoraggio_XDSL | 6 | 366,00 | 2202,01 |
| Servizi di End-Point Management | | Servizio di presidio | 0,6 | 58200,00 | 35015,7 |
| Servizi di End-Point Management | | Servizio di gestione pdl | 90 | 155,50 | 14033,35 |
| Servizi di End-Point Management | | Servizio di gestione stampanti | 10 | 144,00 | 1440 |
| Servizi di End-Point Management | | Secure WEB Getaway | 90 | 10,52 | 949,38 |
| Servizi di Rete e di Sicurezza ICT | | VPN IPSEC NON Gestita | 2 | 717,00 | 1437,9 |
| Servizi di Rete e di Sicurezza ICT | | Start up VPN IPSEC NON Gestita | 0 | 675,00 | 0 |
| Servizi di Rete e di Sicurezza ICT | | Monitoraggio apparato di rete LAN Clienti | 5 | 305,12 | 1529,76 |
| Servizi di Rete e di Sicurezza ICT | | Sicurezza perimetrale presso cliente - Advanced (fino | 1 | 2455,00 | 2461,74 |
| Servizi di Rete e di Sicurezza ICT | | Rete 8 IP | 2 | 321,11 | 643,97 |
| Servizi di Rete e di Sicurezza ICT | | Certificato standard SSL | 1 | 204,88 | 204,88 |
| Servizi di Rete e di Sicurezza ICT | | Domini aggiuntivi (oltre il 1°) per certificato multidoma | 1 | 45,06 | 45,06 |
| Servizi di Rete e di Sicurezza ICT | | Dispositivo OTP: canone annuale per certificato asso | 6 | 3,00 | 18 |
| Servizi di Rete e di Sicurezza ICT | Wifi pubblico - Concentratore bridge | Wifi pubblico - Concentratore bridge | 1 | 2.590,00 | 2590 |
| Servizi Cloud IaaS e PaaS | Gestione e supporto Server Cloud tipologia Linux | Server/apparati | 3,6 | 751,00 | 2703,6 |
| Servizi Cloud IaaS e PaaS | Gestione e supporto Server Cloud tipologia Microsoft | Server/apparati | 8 | 946,26 | 7570,08 |
| Servizi Cloud IaaS e PaaS | Istanza Middleware Jboss - 1 CPU (in aggiunta alla VM c | Istanza | 6,4 | 599,27 | 3835,328 |
| Servizi Cloud IaaS e PaaS | Istanza Middleware Tomcat 1 CPU (in aggiunta alla VM c | Istanza | 1,13 | 148,19 | 167,4547 |
| Servizi Cloud IaaS e PaaS | Sistema Operativo Commerciale per VM e VPC | | 19 | 75,28 | 1430,32 |
| Servizi Cloud IaaS e PaaS | VM (Virtual Machine) - 1 Vcpu (2,67 GHz) | | 23,8 | 148,19 | 3526,922 |
| Servizi Cloud IaaS e PaaS | VM (Virtual Machine) - 1 GB Ram | | 71,14 | 33,72 | 2398,8408 |
| Servizi Cloud IaaS e PaaS | VM (Virtual Machine) - 1 GB Storage prestazionale per VM | | 3985,76 | 0,78 | 3108,8928 |
| Servizi Cloud IaaS e PaaS | DBaaS Oracle DBMS - High Performance - 1 CPU Oracle Ent. (in aggiunta alla VM che ospita il servizio) | | 3,27 | 1639,81 | 5362,1787 |
| Servizi Cloud IaaS e PaaS | DBaaS Oracle DBMS - High Performance - 1 GB RAM Oracle Ent. (in aggiunta alla VM che ospita il servizio) | | 15,35 | 241,96 | 3714,086 |
| Servizi Cloud IaaS e PaaS | 1 GB spazio dati utente per DBMS Oracle | | 2,62 | 6,11 | 16,0082 |
| Servizi Cloud IaaS e PaaS | STASS (Storage As a Service) - 1 GB Spazio Disco Utente | | 5120 | 0,64 | 3276,8 |
| Servizi Cloud IaaS e PaaS | Servizi di condivisione File 1 Utente base e 10 GB spazio disco | | 1 | 38,00 | 38 |
| Servizi Cloud IaaS e PaaS | Servizi di condivisione File 1 Utente aggiuntivo | | 1 | 25,10 | 25,1 |
| Servizi Cloud IaaS e PaaS | Monitoraggio server in Cloud | | 0 | 248,81 | 0 |
| Servizi Cloud IaaS e PaaS | VPC (Virtual Private Cloud) PayPerUse - 1 Vcpu | | 0 | 148,19 | 0 |
| Servizi Cloud IaaS e PaaS | VPC (Virtual Private Cloud) PayPerUse - 1 GB RAM | | 0 | 33,72 | 0 |
| Servizi Cloud IaaS e PaaS | VPC (Virtual Private Cloud) PayPerUse - 1 GB Storage prestazionale per VPC | | 0 | 0,78 | 0 |
| Servizi Cloud IaaS e PaaS | Virtual Network per VPC o VM (1 IP pubblico + 15 RUPAR) | | 0 | 40,13 | 0 |
| Servizi Cloud IaaS e PaaS | STASS Lowrange (Storage As a Service) - 1 GB Spazio Disco Utente | | 342 | 0,48 | 164,16 |